Review of Administration and Expenditure No.13 (2013-2014)

Submission to the Parliamentary Joint Committee on Intelligence and Security

Dr Vivienne Thom
Inspector-General of Intelligence and Security

3 December 2014

Table of Contents

Background

Role of the Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory officer who reviews the activities of the Australian intelligence agencies:

- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Australian Signals Directorate (ASD)
- Australian Geospatial-Intelligence Organisation (AGO)
- Defence Intelligence Organisation (DIO)
- Office of National Assessments (ONA).

In addition to these six agencies the IGIS can be requested by the Prime Minister to inquire into an intelligence or security matter relating to *any* Commonwealth agency. One such inquiry was conducted in 2013-14; it involved ASIO, the Australian Federal Police (AFP) and the Department of Immigration and Border Protection (Immigration).

The overarching purpose of IGIS's activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and is consistent with human rights. A significant proportion of the resources of the office in 2013-14 was directed towards ongoing inspection and monitoring activities, so as to identify issues, including about the governance and control frameworks within agencies, before there is a need for major remedial action. OIGIS staff have access to all documents of the intelligence agencies and the IGIS is often proactively briefed about sensitive operations.

At 30 June 2014 the IGIS was supported by 12 staff and had a budget of $2.18 million.

Details of the activities of the IGIS office are set out in the 2013-14 annual report, available on the IGIS website. This submission highlights relevant issues for the Committee.

Executive Summary

While IGIS oversight is focused largely on the operational activities of the intelligence agencies the Committee may find the outcomes of some IGIS oversight relevant to its review of the administration and expenditure of ASIS, ASIO, ASD, AGO, DIO and ONA. Relevant points arising from oversight activities in 2013-14 include:

- Overall the level of compliance in each of the intelligence agencies is very high. While IGIS inspections and inquiries identify some issues and some others are self-reported by the agencies, these need to be understood in the context of the large and complex operational activities of the intelligence agencies.
- An IGIS inquiry into the attendance of lawyers at ASIO interviews identified a divergence between ASIO policy (which was sound) and the actual practices of some ASIO officers which discouraged the attendance of lawyers at interviews.
- A major IGIS inquiry into the case of an Egyptian irregular maritime arrival identified significant problems in the ways that ASIO and Immigration handled the case and some issues with the passage of information to and from the AFP.
- A review of ASIS use of weapons and self-defence techniques identified issues with controls around weapons and alcohol. An incident that occurred shortly after that inquiry was completed led to a further IGIS inquiry which is ongoing.
- A change to the ASIO practice of allowing staff to search ASIO holdings for records on their neighbours and social contacts occurred after the IGIS raised concerns that the practice was not appropriate and was out of step with community expectations in respect of privacy.
- A small number of ASIS and ASD actions breached the ministerial authorisation and privacy rule requirements in respect of Australians. These were caused by inadequate administrative practices rather than any intention to bypass the rules. The vast majority of activities covered by ministerial authorisation and privacy rule requirements were compliant.

Major inquiries

When undertaking inquiries the IGIS has strong investigative powers, including the power to require any person to answer questions and produce relevant documents. Providing false or misleading evidence is an offence under the *Criminal Code Act 1995*. IGIS inquiries are conducted in private because they almost invariably involve highly classified or sensitive information, and the methods by which it is collected. Inquiry reports go to the relevant agency head, the responsible Minister and, in some cases, the Prime Minister. In most cases an abridged unclassified inquiry report is published on the IGIS website. Conducting an inquiry is resource intensive but provides a rigorous way of examining a particular complaint or systemic matter within an agency.

During 2013-14 the IGIS completed three inquiries. These related to:

- the attendance of legal representatives at ASIO interviews
- the actions of ASIO, the Australian Federal Police (AFP) and the then Department of Immigration and Citizenship in respect of an Egyptian irregular maritime arrival who was placed in immigration detention and was the subject of an Interpol red notice
- ASIS's provision of weapons and weapons and self-defence training to its staff, and the use of weapons and self-defence techniques by ASIS staff.

Abridged versions of each of these inquiry reports are available on the IGIS website.

A new inquiry was initiated following on from the ASIS weapons inquiry and remained open at the end of the reporting period.

Attendance of legal representatives at ASIO interviews

This inquiry was initiated following a complaint alleging ASIO officers had made arbitrary decisions regarding the attendance of legal representatives at security assessment interviews.

The inquiry found that ASIO's internal guidance on attendance of legal representatives at security interviews was both sound and appropriate, and does not preclude the attendance of legal representatives at ASIO interviews. The attendance of legal representatives should be considered on a case-by-case basis, with the default position to allow such attendance.

While the AISO policy was sound I found that, in practice, the attitudes of individual officers, combined with the process established by ASIO and Immigration to arrange interviews, strongly discouraged the attendance of legal representatives. In addition, ASIO differentiated between legal representatives and migration agents, precluding migration agents from attending interviews altogether.

This inquiry led to a number of recommendations. Specifically, ASIO should:

- work with Immigration to ensure arrangements for visa security assessment interviews facilitate the attendance of legal representatives
- improve training in, and staff awareness of, internal policy relating to the potential presence of lawyers at visa security assessment interviews
- clarify the status of any third party wishing to attend a visa security assessment interview to ascertain if they are the interviewee's legal representative, and further consider affording

migration agents the same status as lawyers, with their attendance being addressed on a case-by-case basis
- improve guidance to officers in relation to undertakings of confidentiality.

ASIO agreed to these four recommendations.

I also noted in the report that, in my view, visa applicants should be clearly advised that interviews with ASIO are voluntary. A fifth recommendation was made to adjust the current guidance for staff. This recommendation and some supporting text was afforded a national security classification by ASIO and cannot be publicly released. ASIO agreed, in part, to this recommendation.

At the end of the reporting period ASIO provided advice about the implementation of the recommendations:

- In March 2014, after consultation between ASIO and Immigration, the advice provided by Immigration to visa security assessment interviewees was revised to state that the interviewee is entitled to bring a legal representative.
- ASIO has updated guidance to staff, training and policies relating to visa security assessment interviews. In particular, shortly after the end of the reporting period ASIO finalised a policy on visa security assessment interviews. Training and guidance to staff now reflect the policy position that visa security assessment interviews should commence without efforts to discourage the attendance of a legal representative.
- ASIO's new policy and training requires interviewing officers to clarify the role of a third party seeking to attend a visa security assessment interview to ascertain whether they are the interviewee's legal representative. The presence of migration agents at a visa security assessment interview is considered on a case-by-case basis.
- Revised guidance about confidentiality undertakings addresses the concerns raised in the inquiry.

Inquiry into the management of the case of Mr E

This inquiry was commenced at the request of the then Prime Minister into the way that the AFP, the then Department of Immigration and Citizenship (Immigration) and ASIO handled the case of a particular Egyptian asylum seeker, 'Mr E', who presented complex security issues and, more generally, into the management by Australian government agencies of complex security cases. There had been some media coverage of the case suggesting that Mr E, who was the subject of an Interpol red notice for alleged terrorism offences, was being detained 'behind a pool fence'.

The inquiry found that, although ASIO held information that might have caused it not to clear Mr E for community detention, ASIO's security assessment processes at that time did not include consideration of that information. Different areas of ASIO dealt with the potential match to alerts connected to the Interpol red notice and the community detention checks, and the two areas did not effectively communicate with one another.

Immigration lacked awareness of the types of security checks ASIO conducted and it is not clear that relevant ministers received advice about the rigour of the checks. Within ASIO, guidance provided to staff was inadequate. Operational staff misunderstood the senior executive's intentions and the process of checks conducted differed from that approved by the ASIO executive.

The inquiry found that Immigration made decisions on detention arrangements without a full appreciation of all relevant information. The AFP gave advice to Immigration over a period of time but there was no formal framework for such advice. Information held by separate parts of Immigration was not shared and interpreted consistently. ASIO provided no information to help Immigration assess or manage any detention risks.

The inquiry also found deficiencies in recordkeeping, particularly in Immigration. Key procedures and arrangements between Immigration and ASIO were not well documented.

Significant changes were initiated in ASIO and Immigration prior to this case becoming a matter of public discussion. By the time this inquiry was finished, ASIO and Immigration had introduced considerably more robust security checking processes prior to community detention or the issue of bridging visas, and ASIO had published guidance for staff on how to do the checks and escalate and resolve concerns. Immigration had established a team to identify and oversight national security and serious criminality cases.

At the end of the reporting period the agencies advised me of their progress on implementing the inquiry recommendations.

ASIO noted that it continues to advise Immigration on significant emerging threat issues through providing adverse security assessments and discussing impending assessments where this would assist Immigration's decision making on detention issues. Where ASIO holds information potentially relevant to Immigration's consideration of a person's overall visa suitability, a qualified visa security assessment may be issued. I was provided with a procedural document relating to security assessments for IMAs for whom Immigration is considering the grant or re-grant of a bridging visa, or for those being placed in community detention. This will provide formal guidance for officers in both agencies for handling referrals which potentially match national security alerts.

Inquiries into the use of weapons and self-defence techniques in ASIS

In April 2013, I commenced an inquiry into the use of weapons and self-defence techniques in ASIS. The inquiry was finalised in November 2013. I commenced a further inquiry into the management of weapons in June 2014.

The 2013 inquiry noted that overall ASIS had managed the training in and use of weapons and self-defence techniques well. Two breaches of the ISA occurred between 2004 and mid-2013, both involving the discharge of a firearm without appropriate prior approval. However, both incidents occurred within controlled weapons training environments. In the 2013–14 reporting period there were three further, similar breaches of the *Intelligence Services Act 2001* (the ISA). Recent changes to the ISA mean that the use of a firearm in a 'controlled environment' no longer requires ministerial authorisation.[1]

Two main concerns were identified by the 2013 inquiry. The first was in relation to delays in providing oleoresin capsicum spray and batons to some overseas Stations after this had been approved by the Minister on the basis that the weapons were necessary for the safety of staff. The

[1] Item 16 of Schedule 5 to the *National Security Legislation Amendment Act (No.1) 2014*

inquiry found the delays were due primarily to the lack of central governance of weapons policy and procedures in ASIS.

The second concern related to the consumption of alcohol. ASIS policy at the time required that a person with a blood alcohol content above zero must not be issued with or have carriage of a weapon. The inquiry found some staff misunderstanding in relation to this requirement and that ASIS did not have adequate controls in place to provide assurance that there was compliance with this requirement.

Shortly after that inquiry was completed a further more serious incident occurred overseas involving an allegedly inappropriate action by a member of another Commonwealth agency towards an ASIS officer. Review of the incident confirmed that ASIS did not yet have adequate controls in place to provide assurance that a person with a blood alcohol content above zero would not be issued with or have carriage of a weapon. While no physical injury resulted, the incident had the potential to cause serious injury. ASIS's investigation of the incident highlighted systemic issues. I was advised by the Director-General of ASIS that the investigation also revealed that there were inaccuracies in the information provided to me during the course of my 2013 inquiry. My review of the ASIS investigation report and interviews indicated other substantial discrepancies.

In June 2014 I initiated a further inquiry into the management of weapons by ASIS in that particular overseas location to examine these issues and related matters and to review the findings of my 2013 inquiry report.

Implementation of recommendations from analytic independence inquiry of 2012-13

In 2012–13 I conducted an inquiry into the analytic independence of the assessment activities of ASIO, DIO and ONA. While there was no evidence of inappropriate pressure being placed on any of the agencies, the inquiry recommended a number of improvements to policies, procedures and training in ASIO and DIO.

In early 2014, I conducted a review of DIO's implementation of the inquiry's recommendations. This review found that DIO has made good progress in implementing new policies regarding referencing and recordkeeping and that there had been substantial improvements in the use and quality of references. The review also found improvements in the consistency of recordkeeping. DIO had also implemented new policies regarding key judgment reviews and dissent management.

In mid-2014, I initiated a similar review of ASIO's implementation of the 2012 inquiry's recommendations. This review is expected to be completed by late 2014.

Overview of IGIS inspection program

The office regularly examines selected agency records to ensure that the activities of the intelligence agencies comply with the relevant legislative and policy frameworks and to identify issues before there is a need for major remedial action. These inspections largely focus on the activities of ASIO, ASIS, AGO and ASD given each of these agencies has access to intrusive powers and investigative techniques.

Inspection activities reveal that the vast majority of intelligence agency activities raise no issues of legality or propriety. Some of the areas where concern was identified in the IGIS annual report are noted below. More details on other IGIS inspections are in the IGIS annual report.

ASIO inspection activities

The ASIO Act empowers ASIO to obtain, correlate and evaluate intelligence information relevant to security. ASIO's activities are governed by the ASIO Act as well as the Attorney-General's Guidelines and internal policies and procedures. The Attorney-General's Guidelines require that any means used by ASIO to obtain information must be proportionate to the gravity of the threat and the probability of its occurrence, and inquiries and investigations into individuals or groups should be undertaken using as little intrusion into individual privacy as is possible consistent with the performance of ASIO's functions. Where such intrusions are unavoidable, the distribution of any information obtained should be limited to persons or agencies with a demonstrable 'need to know'.

Routine IGIS inspections in 2013-14 included inspection of:

- Human source management — a considerable improvement in both recordkeeping and compliance with internal ASIO guidelines was noted.
- Submissions to the Attorney-General — these reviews are proving useful in obtaining an overview of legality and propriety issues relevant to high risk activities.
- A selection of investigative cases — this includes looking at the justification and objectives provided for the investigation, whether the investigative activities that were undertaken or proposed were appropriate, whether investigations were subject to formal approval and periodic review, and the application of the principle of proportionality (using less intrusive methods where possible and only progressing to more intrusive methods as required). Our sample selection is oriented to those cases utilising more intrusive investigative methods — for example, cases with warrants approved by the Attorney-General, access to sensitive financial information or prospective data authorisations.

During the reporting period my office sought advice from ASIO on the adequacy of their internal approval procedures for accessing sensitive information from government and non-government agencies. ASIO have advised this issue will be considered in a comprehensive review of their policies and procedures which has recently commenced, and I will be monitoring its progress in this regard.

In one case it was noted that ASIO had provided assistance to a law enforcement agency in response to a request, although that request had not been made by the head of that agency as required under section 19A(2) of the ASIO Act.

Another ongoing focus of my inspections has been to ensure a high standard of recordkeeping and decision making is maintained, particularly in regard to appropriate guidance being provided by authorising officers to more junior staff.

My staff continue to work with ASIO to ensure that the inspection process can provide direct and meaningful feedback to ASIO investigative staff in a timely manner.

Access to ASIO's information holdings by staff

Our inspection program includes the regular review of investigative authorities generated by ASIO for its own internal security purposes.

In one case I questioned whether the justification given for the internal security investigation was sufficient or reasonable, having regard to all of the circumstances. In particular I questioned whether it was appropriate for personal information about a member of the public to be passed to an ASIO officer who had expressed concerns that the individual might pose a risk to the officer's own personal safety.

I was advised at the time that all ASIO staff members could access some ASIO holdings to perform checks on individuals, including neighbours and social contacts that might relate to personal security or safety. I expressed concern that ASIO did not have formal processes in place to ensure that personal information in ASIO's holdings about a member of the public could not be released to a staff member or accessed directly by the staff member. In my view, this is out of step with community expectations in respect of privacy.

In response to the concerns I raised, in June 2014 ASIO implemented a new security policy for the use of information holdings within ASIO. The policy emphasises that information holdings within ASIO are only for official purposes and that ASIO staff are not to access ASIO information holdings to obtain information which may be relevant to their personal circumstances. Staff with security concerns should raise this with the relevant area within ASIO, which will conduct the necessary checks.

In my view this is a significant improvement in privacy protection that occurred as a result of concerns raised by this office. I will be monitoring the implementation of this new policy and have requested that ASIO provide details of any post-implementation audits.

ASIO warrants

In 2013-14 IGIS staff reviewed around half of all warrants obtained by ASIO, these inspections usually occur after an operation has been completed. In the majority of cases no issues of legality or propriety were identified with the warrants. Four errors were identified in inspections. In addition ASIO self-reported three breaches of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and two breaches of the *Australian Security Intelligence Organisation Act 1979*. Most breaches of the TIA Act resulted from errors by a carrier, not by ASIO. ASIO issues with warrants included delay in revocation, configuration errors and administrative errors. Further details are in the IGIS annual report.

There was a modest increase in the number of 'B-Party' warrants during the reporting period, following a decrease in the previous year. B-Party warrants are warrants that allow the interception of the communications of a person who is not believed to be engaged in activities prejudicial to security in order to capture the communications of another person who is.

The *Cybercrime Legislation Amendment Act 2012* came into effect in late 2012. This Act amended the TIA Act to provide a new power for ASIO and law enforcement agencies to give notice to telecommunications carriers to require them to retain certain stored communications for up to 90 days while ASIO seeks an appropriate warrant to access those communications. Throughout the

reporting period there were a very small number of such notices raised by ASIO. No issues of concern were identified in relation to those reviewed by IGIS.

ASIO access to telecommunications location information or subscriber data

The TIA Act provides the legal authority for a nominated group of ASIO senior managers to authorise collection of prospective and historical telecommunications data from telecommunications carriers or carriage service providers. Prospective data authorisations provide near real-time location and other subscriber information for the period that an authorisation is in force. The threshold that ASIO is required to meet is that access to the data is in connection with the performance by ASIO of its functions. In addition, the Attorney-General's Guidelines state that investigative activities should use as little intrusion into personal privacy as is possible , consistent with the performance of ASIO's functions. A request for access to telecommunications data should only be submitted once less intrusive methods have been attempted, or considered and found to be insufficient. Similarly, the Attorney-General's Guidelines state that authorisation levels for activities should be higher for more intrusive investigative techniques.

ASIO's access to prospective telecommunications data is reviewed as part of our regular inspection programme. Due to their intrusive nature, access to prospective and historical telecommunications data are reviewed in a similar manner to telecommunications warrants.

I did not identify any concerns with ASIO's access to prospective and historic telecommunications data. My office's oversight of this particular investigative technique decreased during this reporting period due primarily to changes in our inspection program and the high rate of compliance in this area.

I am satisfied that prospective data authorisations reviewed were endorsed by an appropriate senior officer, and that ASIO has regard to the Attorney-General's Guidelines and is meeting the legislative requirement to only make requests for data in connection with the performance of its functions.

Exchange of information with foreign liaisons

The ASIO Act provides the authority for ASIO to seek information from, and provide information to, authorities in other countries that is relevant to Australia's security, or the security of the foreign country. ASIO may only cooperate with foreign authorities approved by the Attorney-General. In general, the types of foreign authorities approved by the Attorney-General perform broadly similar functions to ASIO, and include security and intelligence authorities, law enforcement, immigration and border control, and government coordination bodies.

ASIO has internal guidelines that govern the communication of information on Australians and foreign nationals to approved foreign authorities. These guidelines impose an internal framework for assessing and approving the passage of such information. ASIO's internal requirements vary according to the country, based on factors such as ASIO's previous experience dealing with their authorities and how the foreign authorities manage information received, including in relation to human rights issues.

During 2013–14, my office inspected a sample of authorisation documentation and correspondence for such exchanges, both through regular reviews of ASIO investigative cases and through dedicated foreign liaison inspection activities.

My office identified one instance when ASIO communicated information on Australian persons to a non-approved foreign authority responsible for issuing passports for that country. The case raised complex legal issues and at the end of the reporting period I had not formed a final view on whether approval from the Attorney-General was strictly legally required; however, my view is that at least as a matter of propriety and compliance with the intention of the restrictions the matter should have gone to the Attorney-General.

Inspections by my office have also identified cases where ASIO could improve compliance with internal guidelines, particularly in relation to documenting human rights considerations. I continue to raise these matters with ASIO.

Inspection of agencies subject to the *Intelligence Services Act 2001*

Limits on intelligence agencies' functions

The functions of the ISA agencies are set out in sections 6, 6B and 7 of the ISA. For example, for ASIS the most relevant functions are to obtain *in accordance with the Government's requirements,* intelligence about the capabilities, intentions of activities of people or organisations outside Australia; and to communicate *in accordance with the Government's requirements*, such intelligence. The work of ASIS, ASD and AGO is guided by the national intelligence priorities, which are reviewed and agreed by the National Security Committee of Cabinet each year.

The ISA also requires that ASIS, ASD and AGO only perform their functions in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.

While I do not conduct particular inspections to determine whether agencies' activities comply with the limits of their functions, we are always mindful of this fundamental question. In most cases it is clear how particular intelligence products relate to the national intelligence priorities.

Ministerial authorisations

Any activity to produce intelligence on an Australian person by Australia's foreign intelligence collection agencies requires ministerial authorisation. Ministers may also direct that other activities require prior ministerial approval. In the case of Australian persons who are, or are likely to be, involved in activities that pose a threat to security, the approval of the Attorney-General must also be obtained. In AGO's case, any intelligence collected over Australian territory requires authorisation by the head of the agency.

Privacy rules

Section 15 of the ISA provides that the ministers responsible for ASIS, ASD and AGO must make written rules to regulate the communication and retention of intelligence information concerning Australian persons (privacy rules). The term 'Australian person' generally includes citizens,

permanent residents and certain companies. These rules regulate the agencies' communication of intelligence information concerning Australian persons to other Australian agencies and to foreign authorities including to Australia's closest intelligence partners. (Communication to foreign authorities is also subject to additional requirements.)

Privacy rules require that agencies may only retain or communicate information about an Australian person where it is necessary to do so for the proper performance of each agency's legislatively mandated functions, or where the retention or communication is required under another Act.

If a breach of an agency's privacy rules is identified, the agency in question must advise my office of the incident, and the measures taken by the agency to protect the privacy of the Australian person, or Australian persons more generally. Adherence to this reporting requirement provides me with sufficient information upon which to decide whether appropriate remedial action has been taken, or further investigation and reporting back to my office is required.

The presumption of nationality

The privacy rules require that ASIS, ASD and AGO are to presume that a person located in Australia is an Australian person, and that a person who is located outside of Australia is not an Australian person unless there is evidence to the contrary.

An agency may later overturn an initial presumption of nationality, for example:

- New information or evidence may indicate that a person overseas is an 'Australian person'. If it was not reasonable for this information to have been known and considered at the time the initial assessment was made then the presumption of nationality could be overturned but there would have been no breach of the privacy rules.
- The agency may discover that it was already in possession of evidence that indicated that a person was an Australian person that should have been considered in the initial assessment, or another Australian agency might have possessed that information. In this case the presumption of nationality would be overturned but, if intelligence information had already been communicated about the Australian person, there could have been a breach of the privacy rules.

If the agency made a reasonable assessment of the nationality status of that person, based on all information which was available at the time, there is no breach of the privacy rules but the case must still be reported to me.

Where a presumption of nationality is later found to be incorrect ASIS, ASD and AGO must advise my office of this and the measures taken to protect the privacy of the Australian concerned.

Inspection of ASIS activities

Ministerial authorisations

There was a significant improvement in ASIS's compliance with ministerial authorisation requirements during late 2013, compared to 2012–13 when a number of issues had been identified; however, a number of breaches of the ISA in relation to ministerial authorisations occurred in the first half of 2014.

In April 2014 ASIS advised my office of a breach where an ASIS officer collected information by searching the personal property of an Australian person without ministerial authorisation.

Section 10A of the ISA requires the Director-General of ASIS to report to the Minister for Foreign Affairs on the authorised activities within three months of the day on which the relevant authorisation ceased to have effect. There were three breaches of section 10A of the ISA:

- an inspection by my office identified one occasion where a report on an authorisation that had expired had been submitted outside the three month period
- ASIS advised my office of two occasions when ASIS failed to submit a report within three months of the authorisations ceasing to have effect.

My staff also identified one occasion where ASIS failed to inform the minister when the grounds on which an authorisation was issued ceased to exist as required by s 10(2A) of the ISA.

Protecting the privacy of Australian persons

We meet with ASIS staff every two months to discuss compliance with privacy rules and undertake inspections of ASIS's dissemination of information about Australian persons.

In 2013–14 ASIS reported eight occasions where the presumption of nationality was overturned; that is, information came to light that an individual was actually an Australian person and the privacy rules were applied retrospectively to reporting. On more than one of these occasions there was initial inconsistency between the views of ASIS and ASD on whether a person was an Australian person. I have advised all agencies that it is important that agencies take a consistent approach to the presumption of nationality, to avoid a situation where agencies draw separate conclusions as to the nationality of a particular individual. In seven of these cases the initial presumption of nationality had been reasonable and there was no breach of the privacy rules.

In August 2013 ASIS advised me that a March 2013 report had failed to take account of the fact that the individual concerned was an Australian citizen (with dual nationality) and thus the communication breached the privacy rules. At the time, the notification was limited to advice about the communication of intelligence. There was no notification about the collection of intelligence.

When ASIS provided further information about the case in March 2014 I raised a concern as to whether:

- the collection and passage of information in relation to this individual had adhered to the ISA's 'requirement that intelligence only be communicated in accordance with the Government's requirements' (s.6(1)(b))
- there had been unauthorised collection against the individual breaching the ISA's requirement that ASIS 'obtain ministerial authorisation before undertaking any activity to produce intelligence on an Australian person' (s.8) after ASIS first became aware of the individual's dual nationality in July 2012.

ASIS investigated the case further. I received a copy of the final report from the Director-General in June 2014, which confirmed there had been a breach of both section 6(1)(b) and section 8 of the ISA, as well as a breach of the privacy rules. The Director-General directed that remedial action include:

- further checks to determine whether there had been any other breaches of section 6(1)(b)
- updated guidelines, training and advice to staff on the issue, including on the requirement for ministerial authorisations for Australian persons
- a review of systems, processes and procedures relating to the application of privacy rules
- a code of conduct and other investigations as necessary to determine appropriate action in relation to the individuals responsible for the breaches.

I will monitor the implementation of these actions.

ASIS also reported two occasions where there were breaches because the privacy rules were not applied to reporting on a person known to be an Australian person. Inspections by my office identified an additional two breaches where the privacy rules had not been applied. ASIS subsequently amended all four reports and applied the privacy rules retrospectively.

Review of operational files

ASIS activities often involve the use of human sources and ASIS officers are deployed in many countries to support a wide range of activities including counter-terrorism, efforts against people smuggling and support to military operations. These activities are often high-risk and sensitive. During the reporting period, we reviewed files relating to operational activities in a diverse range of countries where ASIS has a presence.

While the sensitive nature of ASIS's operational activities means that I cannot specifically detail the nature and range of issues arising from these inspections in a public report, I can advise that these reviews are thorough and rigorous and something in which I take a keen personal interest. No significant issues were raised during the reporting period as a result of these inspections.

Authorisations relating to the use of weapons

Schedule 2 of the ISA requires the Director-General of ASIS to provide the IGIS with:

- copies of all approvals issued by the Minister of Foreign Affairs in respect of the provision of weapons and the training in and use of weapons and self-defence techniques in ASIS
- a written report if a staff member or agent of ASIS discharges a weapon other than in training.

This reporting requirement was met during 2013–14 and I am satisfied that the need for limited numbers of ASIS staff to have access to weapons for self-defence in order to perform their duties is genuine. I am also satisfied that appropriate controls are in place to limit the circumstances in which weapons may be used for self-defence.

An inspection of records relating to the provision by ASIS of training in the use of self-defence techniques and weapons was conducted in May 2014. It was apparent that governance and recordkeeping improvements implemented in the previous reporting period were proving effective.

The May 2014 inspection confirmed one breach of the ISA, where an ASIS officer who had not been approved for training in or the use of weapons discharged a firearm in a skills maintenance session in March 2014. This incident had already been brought to my attention by ASIS. ASIS reported a further two breaches of the ISA relating to the unapproved use of weapons by ASIS officers during the reporting period; one at a skills maintenance session in September 2013 and one at a firing

range in December 2013. I note that recent legislative amendments mean that the use of weapons in such circumstances will no longer require ministerial authorisation.

Inspection of ASD activities

OIGIS staff members have access to and ongoing visibility of ASD's activities. We undertake regular inspections on a range of ASD activities, with a particular focus on the privacy of Australians. More generally, staff may inspect any activity undertaken by ASD, with regard to legality and propriety, and whether the activities are consistent with human rights. The legality of any ASD activity is assessed by reference to whether the purpose was consistent with a function of ASD, whether it was within the limits set out in the relevant legislation, and whether the activity had an appropriate level of approval.

ASD can only cooperate with an authority of another country to the extent authorised by the Minister for Defence. These authorising instruments are reviewed by my office.

Ministerial authorisations

During 2013–14, OIGIS staff continued to review all ministerial authorisations presented to the Minister for Defence. Overall, I observed a high level of compliance with authorisations and relevant directions issued to ASD by the minister.

Throughout 2013–14, I continued to monitor records of intelligence collection activities undertaken by ASD under ministerial authorisations. Following the implementation of a number of improved governance and administrative arrangements in ASD in mid-2013, I observed a significant improvement in the agency's ability to self-identify and appropriately respond to compliance risks during the reporting period.

We also conducted a small number of non-routine spot checks and inspection projects to assess how ASD deals with targets where there is a higher than usual compliance risk. These inspections demonstrated a high level of understanding by ASD staff of legislative requirements and thresholds for undertaking activities under the ISA and the ASIO Act.

In August 2013, I completed a review of an incident which came to my attention in mid-2013, involving a breach of the ISA where intelligence targeting occurred for several days after ASD had determined the target to be an Australian person. While I found no evidence of intentional wrongdoing, my review highlighted a number of compliance concerns in relation to the event and ASD's handling of the matter.

ASD subsequently initiated an investigation into the incident and identified a number of areas for improvement in its internal policy framework and procedures. ASD has kept my office informed of progress on the implementation of revised procedures, and I am satisfied that action taken in response to my original concerns is appropriate.

In January 2014, ASD separately provided to me their final report on a breach of the ISA which occurred during October 2013, where incomplete records had resulted in ASD conducting intelligence collection activity on a person known to be Australian.

During the reporting period I continued to inspect cancellations of ministerial authorisation and non-renewal reports to the Minister for Defence under sections 10 and 10A of the ISA. In September

2013, as part of our regular inspection of ASD activities, I asked ASD to confirm that intelligence collection against several subjects had ceased (as had been advised by ASD to the Minister for Defence). ASD advised that collection against one subject had continued for several months beyond the expiry of the ministerial authorisation, in breach of the requirements specified in the ISA.

This finding in September 2013 contributed to a decision by ASD to consider its quality assurance processes for managing specific types of ministerial authorisations. In late 2013, ASD initiated a thorough retrospective analysis of cancelled or expired ministerial authorisations. This review is discussed below under *Legacy incidents: review of ministerial authorisation cancellations and non-renewals*.

Protecting the privacy of Australians

In accordance with their obligations, ASD continued to report to me cases where a presumption of nationality had later been found to be incorrect, and the measures taken to protect the privacy of the Australian person. I found the actions taken by ASD in response to incorrect presumptions of nationality occurring during the reporting period, including the timely notification to other intelligence agencies, to be generally appropriate.

In two cases there were breaches of the privacy rules as the presumption of nationality was not applied reasonably by ASD. In both cases, intelligence collection activity occurred against Australian persons in circumstances where ASD already had information indicating that the individuals concerned were Australian persons, but in each case members of staff had failed to make appropriate inquiries of existing ASD records. In addition to these cases being breaches of the presumption rule in the privacy rules, the action taken to produce intelligence on an Australian person was inconsistent with the ministerial authorisation requirement in the ISA.

During 2013–14, I assessed two instances where ASD communicated information about an Australian person not in accordance with the privacy rules. Both incidents resulted from a failure to follow established compliance processes. I am satisfied the remedial action taken in both cases appropriately addressed the privacy of the Australian persons concerned.

The privacy rules and cooperation with signals intelligence partners

ASD works particularly closely with a small number of allied signals intelligence agencies. During the reporting period, ASD reported to me several instances where it had identified that one of these partner agencies had made an incorrect presumption of nationality, and had inadvertently communicated information on an Australian person. I was satisfied that ASD followed up with partner agencies concerning any required remedial action in a timely and appropriate manner.

Inspection project involving ASD

In January 2014, I initiated an inspection project into specific activities of ASD conducted in response to a high-priority collection effort directed by government. The project found a high level of compliance by ASD in relation to:

- obligations imposed by ministerial authorisations and ministerial directions issued under the ISA
- intelligence reporting and dissemination
- coordination between ASD and other Australian intelligence agencies, and

- actions taken to protect the privacy of Australian persons.

In a small number of the cases investigated, ASD staff did not consistently follow established recordkeeping requirements. While there was no breach in these cases, I note that a number of compliance incidents involving breaches of the ISA over the previous year had also resulted from a failure to adhere to recordkeeping requirements, thereby constituting a significant compliance risk.

Consistent with routine inspections of ASD, and reviews conducted internally by ASD of compliance incidents, the project findings highlighted the importance of best practice corporate recordkeeping for ensuring high levels of compliance. At the end of the reporting period, ASD advised it was updating a number of compliance frameworks which will help increase staff understanding and minimise compliance risks in similar cases.

Compliance with the *Telecommunications (Interception and Access) Act 1979*

ASD brought to my attention one case where a ASD officer who was assisting with the execution of a warrant had not been listed as an authorised person for the purpose of exercising the authority of a warrant in respect of a telecommunications service. ASD took remedial action immediately upon learning of the error. I am satisfied that ASD's actions were appropriate and that this error was administrative in nature. Recent changes to legislation allow authorisations by class of officer and will reduce the likelihood of any future breaches of this nature.

Monitoring AGO

During 2013–14 we conducted several inspection visits to AGO, in addition to access to AGO's online records of its collection activities. As in past years, this office focused on AGO's compliance with the terms of each ministerial authorisation issued to the agency by the Minister for Defence, noted the time taken to cancel collection activities when the grounds for the ministerial authorisation had materially changed, and reviewed the accuracy of reports provided to the Minister for Defence following the expiry or cancellation of a ministerial authorisation.

OIGIS staff also closely examined the adequacy of AGO's attempts to determine the nationality of individuals or entities before initiating targeted collection activities (to establish whether or not a ministerial authorisation was required). We also examined the extent of cooperation between AGO and other intelligence collection agencies when seeking intelligence about the same target or requesting a joint ministerial authorisation.

No significant errors or breaches were identified. Based on these inspection activities, I am confident AGO takes its statutory obligations under the ISA seriously and has put in place robust systems to encourage compliance.

My staff and I discussed specific compliance issues with the Director AGO and with relevant AGO officers at several meetings.

Monitoring DIO and ONA

As has been the practice of this office over many years, we continue to exercise a 'light touch' approach to the activities of ONA and DIO. As these agencies do not collect covert intelligence, their activities are far less likely than those of the collection agencies to intrude upon the personal affairs of Australian persons.

We aim to review ONA and DIO's compliance with their privacy guidelines at least twice a year. In 2013–14 we undertook two inspection visits to DIO and one to ONA. A further visit to ONA planned for June 2014 was postponed to the next reporting period due to other IGIS priorities.

These inspections revealed that ONA and DIO are generally compliant with the requirements of their privacy guidelines and that they each take their privacy responsibilities seriously. The few non-compliance issues identified tended to be questions of nuance or administration, rather than whether or not relevant intelligence information about Australian persons or entities should be included in their products.

My staff also engaged with ONA and DIO on wider Australian intelligence community issues and, in the case of the Public Interest Disclosure scheme, to gather information relevant to the Commonwealth Ombudsman.

My office also conducted a thorough review of DIO's implementation of recommendations from a 2012 inquiry examining DIO's analytical integrity.

Cross-agency inspections

Use of assumed identities

Part 1AC of the *Crimes Act 1914* and corresponding State and Territory laws enable ASIO and ASIS officers to create and use assumed identities in carrying out their functions. The legislation protects authorised officers from civil and criminal liability where they use an assumed identity in a circumstance that would otherwise be considered unlawful. Similarly, the legislation provides protections to the Commonwealth, State and Territory agencies responsible for providing the evidence of an assumed identity in this context.

The legislation also imposes reporting, administration and audit regimes on those agencies using assumed identities. ASIO and ASIS are required to conduct six-monthly audits of assumed identity records and provide the IGIS with an annual report containing information on the assumed identities created and used during the year. The Director-General of Security and the Director-General of ASIS provided reports covering the activities of their respective agencies for the 2012–13 reporting period. Nothing in the reports caused me concern.

This year, my staff also inspected ASIS's assumed identity records. No issues of concern were identified during the inspection, and I was satisfied that ASIS is complying with Commonwealth, State and Territory legislation. I have asked ASIS to provide me with copies of their internal audit reports in addition to the annual report in future, as is ASIO's current practice. Provision of this additional level of detail will strengthen existing oversight mechanisms.

ASIS advised of a breach of its internal policy in 2014 where equipment was purchased without first obtaining an assumed identity. This was due to human error: a staff member did not understand the requirements. ASIS have put procedures in place to ensure this does not happen again.

Access to sensitive financial information by intelligence agencies

The *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (the AML/CTF Act) provides a legal framework in which designated agencies are able to access and share financial intelligence information created or held by the Australian Transaction Reports and Analysis Centre (AUSTRAC).

All intelligence agencies and the office of the IGIS are designated agencies for the purposes of the AML/CTF Act.

The IGIS is party to an MOU with AUSTRAC. This MOU establishes an agreed understanding of IGIS's role in monitoring agencies' access to, and use of, AUSTRAC information.

In oversighting the agencies' use of AUSTRAC information, we check that there is a demonstrated intelligence purpose pertinent to the agencies' functions, that access is appropriately limited, searches are focused, and information passed to both Australian agencies and foreign intelligence counterparts is correctly authorised.

ASIO

Early in the reporting period I finalised my annual statement for 2012–13 to the Attorney-General on the outcome of my compliance monitoring activities in ASIO, concerning access to, and use of, AUSTRAC information in the previous reporting period.

I noted that ASIO was not compliant with AUSTRAC's guidelines on the storage of certain AUSTRAC information. ASIO subsequently began negotiations with AUSTRAC to reach a solution and has since been provided with a waiver from the CEO of AUSTRAC in respect of the storage requirements on the condition that ASIO implement internal user access controls to this sensitive information.

During my 2013–14 inspection program, a breach of Section 133(1) of the AML/CTF Act was identified whereby ASIO communicated AUSTRAC information to a foreign intelligence agency without first receiving appropriate undertakings for the protection and use of the information. This breach will be included in my next annual statement to the Attorney-General.

ASIS

Early in the reporting period I finalised my annual statement for 2012–13 to the Minister for Foreign Affairs on the outcome of my compliance monitoring activities in ASIS, concerning access to, and use of, AUSTRAC information in the previous reporting period.

In that annual statement I noted two areas of shortcoming in 2012–13; the first in relation to the accurate receipt of AUSTRAC information within ASIS and the second regarding deficiencies in relation to reporting movements of currency into or out of Australia.

Inspections by my office throughout 2013–14 have indicated that shortcomings by ASIS in relation to recordkeeping have continued and this will be included in my statement to the Foreign Minister. No deficiencies regarding movements of currency into or out of Australia were observed in 2013–14.

Complaints to the IGIS office

The IGIS office receives complaints from members of the public as well as current and former Commonwealth officials.

In 2013–14, IGIS received a total of 504 complaints, of which 487 were about visa-related security assessments and 17 were non visa-related. Most non-visa related complaints are related to employment matters, often from current or former intelligence officials.

Visa security assessments

The largest number of complaints came from individuals seeking skilled business and work visas, or family reunion visas. Complaints from irregular maritime arrivals (IMAs) comprised only 9.5 per cent of complaints actioned by my office.

Most visa security assessment complaints concern delay. In cases where the visa application was lodged more than 12 months previously, we examined ASIO's systems to determine whether or not the applicant had been referred to ASIO for a security assessment and, if so, reviewed ASIO's handling of the matter. In each case, we looked at whether ASIO had acted unreasonably or had made a processing error. The rate of ASIO error is low.

My office does not undertake a merits review of adverse or qualified security assessments. An Independent Reviewer of Adverse Security Assessments has been engaged by the Attorney-General's Department to conduct an advisory review of adverse security assessments in relation to individuals who are in immigration detention and have been found to be owed protection obligations under international law.

Employment related complaints

Most employment related complaints from current or former intelligence officers concern revocation of security clearances leading to termination of employment. A small number of complaints were also received from individuals who had their 'arrangements' with ASIS terminated.

Complaints were also made about ASIO delay in finalising Aviation Security Identification Cards (ASIC) and Maritime Security Identification Cards (MSIC). ASIO processes most ASIC and MSIC requests quickly, a small number of more complex cases can take a long time to resolve.

Public Interest Disclosure Scheme

The Public Interest Disclosure (PID) scheme commenced on 15 January 2015. All of the intelligence agencies had procedures and policies in place for the commencement of the scheme.

At the end of the reporting period the IGIS office had received one direct disclosure that fell within the parameters of the PID scheme and had been advised of six PID cases that had been allocated across the intelligence agencies. Cases have mostly involved personnel management matters. One case involved administrative deficiencies in the procurement of external services, and the agency concerned has advised that investigation of this disclosure identified useful refinements to administrative processes.

The year ahead

2014-15 has already seen significant changes to the powers of intelligence agencies. These agencies have also received extra resources.

The IGIS office has also received approximately $0.8 million in additional funding and is in the process of recruiting up to five more staff. It is expected that the total staffing of the office will be 16 by the end of 2014-15; but this number would decrease over time with any efficiency dividend. The annual budget of the office is now $3 million.

Significant areas of focus for the IGIS office in 2014-15 include:

- the introduction of an oversight program for ASIO special intelligence operations
- inspections of ASIO warrants, particularly the new computer access warrants and identified person warrants
- the use of surveillance devices without warrant by ASIO
- ASIS activities against Australian persons in support of ASIO (which no longer require ministerial authorisation in most cases)
- ASIS activities in support of military operations (which will be able to be authorised by a class authorisation)
- scrutiny of any emergency authorisations given by agency heads
- examining ASIO training and procedures for the new power to use of force against persons
- ASIO actions in relation to the suspension and cancellation of travel documents
- participation in the review of the Attorney-General's Guidelines issued under s8A of the ASIO Act, including requirements that govern ASIO's management and destruction of information obtained on persons who are not relevant, or are no longer relevant, to security matters[2]
- reviewing ASIO implementation of recommendations from the 2012 analytic independence inquiry
- ongoing inspection and complaint management, including in relation to adverse security assessments.

[2] Recommendation 4 of the PJCIS *Advisory Report on the National Security Legislation Amendment Bill (No.1) 2014*