Review of Administration and Expenditure No.14 (2014-2015)

Submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone
Inspector-General of Intelligence and Security

20 January 2016

Table of Contents

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.

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 acts consistently with human rights. A significant proportion of the resources of the office in 2014-15 continued to be 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.

During 2014-15, the IGIS received additional funding and an exemption from the efficiency dividend. The budget funding for the IGIS office for 2014-15 was $2.2 million, and the budget for 2015-16 is $3.05 (including additional funding and the effect of the efficiency dividend). The additional funding has allowed the IGIS to recruit an additional five staff. At 30 June 2015 the IGIS was supported by 16 staff.

Details of the activities of the IGIS office are set out in the 2014-15 annual report, available on the IGIS website. This submission highlights relevant issues for the Committee.

Executive Summary

During 2014-15, the Parliament passed a number of pieces of national security legislation, which included new and amended powers for some of the AIC agencies. The legislation included:

- *National Security Legislation Amendment Act (No. 1) 2014*
- *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014*
- *Counter-Terrorism Legislation Amendment Act (No.1) 2014*
- *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*

The IGIS office received additional funding in recognition of increased oversight responsibilities as a result of the above legislation. This enabled recruitment of five additional staff to the office. Further, the Government decided to exempt IGIS from the efficiency dividend, which otherwise would have had to be met by gradually reducing staffing.

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 in 2014-15 include:

- An inquiry into the management of weapons by ASIS in a specific location was completed.
- An inquiry into certain actions of ASD was initiated and was close to finalisation at the end of the reporting period.
- The IGIS office continued its program of regular inspection of agency records. During 2014-15, particular focus was given to inspection of the agencies' use of new and amended powers, such as special intelligence operations, identified person warrants and ASIS activities to assist ASIO obtain intelligence on Australian persons that do not require a ministerial authorisation.
- Overall the level of compliance in each of the intelligence agencies continued to be very high. While IGIS inspections and inquiries identified some issues and some others were self-reported by the agencies, these need to be understood in the context of the large and complex operational activities of the intelligence agencies.

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 is a rigorous way of examining a particular complaint or systemic issue within an agency.

During 2014-15 the IGIS completed an inquiry into the management of weapons by ASIS in a specific location. The report of the inquiry made 13 recommendations, and ASIS agreed to all of the recommendations. Some of the steps taken by ASIS to address areas of concern include:

- the establishment of a compliance branch;
- an extensive compliance outreach training program;
- widespread consultation with staff;
- a review of all ASIS policy and procedures, to be made centrally available on a new platform.

During 2014-15 the IGIS initiated an inquiry into certain actions of ASD. The report of this inquiry was finalised shortly after the end of the reporting period.

Implementation of recommendations from the 2013 inquiry in relation to ASIS use of weapons

During 2014-15 ASIS finalised the implementation of IGIS recommendations arising from the 2013 Weapons Inquiry. This included:

- updated weapons related standard operating procedures for all stations where ASIS staff are or may be issued with weapons;
- revised ASIS Guidelines for the use of weapons and self-defence techniques;
- a review of operational environments to identify stations that require weapons and self-defence training;
- new safeguards and controls implemented in all stations where ASIS staff are or may be issued with weapons.

Implementation by ASIO of recommendations from analytic independence inquiry of 2012-13

In 2012–13 the IGIS conducted an inquiry into the analytic independence of the assessments made by 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, ASIO invited the former Director-General of ONA, Mr Allan Gyngell AO, to conduct a comprehensive review into the state of analytic tradecraft and practices supporting the assessment function in ASIO. Shortly after Mr Gyngell's review, the IGIS initiated a review of ASIO's implementation of the 2012 inquiry's recommendations. At the time of the review, ASIO was in the process of developing and trialling new organisation-wide policies. The review noted that there

remained inconsistency in relation to ASIO analytic tradecraft, but the adoption of the organisation-wide policies was expected to lead to improvements. In June 2015, ASIO advised that the policies had been endorsed and were now being implemented across the Organisation. Adoption of this policy across relevant areas of ASIO should address the areas identified for improvement raised in the inquiry. IGIS will monitor this area through future inspections.

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 potential problems before there is a need for major remedial action. These inspections largely focus on the activities of ASIO, ASIS, ASD and AGO 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 notable inspections or 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 *Australian Security Intelligence Organisation Act 1979* (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 that 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 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 of ASIO records in 2014-15 included inspection of:

- a selection of investigative cases;
- submissions to the Attorney-General;
- human source management.

The IGIS also implemented a number of new inspections in response to the various legislative amendments during the reporting period. These included:

- ASIO warrants. Warrants are usually reviewed as part of the inspection of investigative cases. In order to provide close scrutiny of ASIO's use of the new and amended warrants under the ASIO Act, in 2015 we reviewed a sample of relevant warrants each quarter. The new identified person warrants were a particular focus because under the warrant authorisations to use particular powers can be granted by the Director-General (or the

Attorney-General). As the Director-General is now able to authorise the use of powers that would previously have required the Attorney-General's approval, I consider close scrutiny by our office is appropriate. Of the identified person warrants inspected during the reporting period, the majority of authorisations to use specific powers were given by the Director-General.

- Special Intelligence Operations (SIOs). These involve a new power available to ASIO since October 2014. SIOs are similar to law enforcement 'controlled operations', as they enable the Attorney-General to authorise a person to engage in conduct that would otherwise be unlawful. The office established an inspection program to review each SIO authorised by the Attorney-General.
- Passport suspensions and emergency visa cancellations. In 2014 Parliament also passed laws enabling Australian and foreign passports to be suspended on security grounds for 14 days, and for the emergency cancellation of visas for 28 days. The suspension or cancellation is triggered by advice from ASIO, and enables action to be taken pending more detailed consideration by ASIO as to whether there are grounds to issue an adverse security assessment recommending passport or visa cancellation. As the thresholds for suspension or emergency cancellation are lower than for regular passport or visa cancellation, and merits review by the AAT is not available, the office has established an inspection program to review these cases and ensure ASIO's actions and advice are appropriate based on the information available to it at the time.

Use of force

One of the amendments made by the *National Security Legislation Amendment Act (No. 1) 2014* was to provide that warrants issued under the ASIO Act must authorise the use of any force against persons or things that is necessary and reasonable to do the things specified in the warrant. The ASIO Act did not previously authorise the use of force against persons, and the IGIS therefore considered this to be a new power. The PJCIS recommended that the IGIS provide close oversight of the design and execution of training for ASIO officers who may be required to use force during the execution of warrants issued under the ASIO Act. There has been consultation between ASIO and the IGIS in relation to training and ASIO policy guidance. At the end of the reporting period, ASIO had commenced a self-defence training program, and was looking at developing additional training specifically for officers involved in the execution of warrants.

The IGIS is required to be notified if force is used against a person under an ASIO warrant. During the reporting period, the IGIS received one such notification. The force was exercised by law enforcement officers assisting ASIO in the execution of the warrant. There was no indication in the police report regarding the use of force that it was other than reasonable and proportionate for the purpose for which it was executed. The timeliness of ASIO providing notification to the IGIS of any use of force was the subject of comment in the IGIS Annual Report.

ASIO access to telecommunications data

During the reporting period, Parliament passed the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* ('Data Retention Act'). The substantive provisions of that Act commenced on 13 October 2015. The scheme requires carriers to retain specified data for at least two years. The Act also established requirements for warrants to be obtained before an agency

requests access to telecommunications data of a journalist for the purpose of identifying the journalist's source.

The IGIS inspects ASIO's access to historical and prospective telecommunications data through our existing inspections. We will continue to monitor this area, having regard to the Data Retention Act, but this will not require substantial modification of existing inspection activities.

The IGIS 2014-15 Annual Report made several comments with regards to ASIO's access to historical and prospective data:

- the prospective data authorisations reviewed showed appropriate approval by senior officers demonstrating that ASIO had regard to the Attorney-General's Guidelines;
- a small number of errors in compliance with ASIO's internal approval were identified in requests for historical telecommunications data;
- some requests for access to prospective telecommunications data did not adequately explain why less intrusive methods of obtaining the information had not been pursued or would not be appropriate.

Inspection projects

In addition to regular inspection activities, from time to time the IGIS initiates inspection projects that focus on a particular issue or area. During the reporting period, ASIO-related inspection projects included:

- ASIO's investigations of issues-motivated groups;
- passport cancellations;
- whole of life warrants;
- ASIO internal approval processes;
- ASIO's record retention and destruction;
- ASIO requests for information from Intelligence Services Act agencies.

ASIO's investigations of issues-motivated groups

This inspection project did not arise from any complaint or concern, but was initiated on the basis that it is an area of consistent public and media interest, and was particularly relevant in light of the Brisbane G20 summit held in November 2014.

The project found that the overall scale of ASIO's investigation of groups and individuals that may be associated with issues-motivated groups appeared to be reasonable and justified in the context of ASIO's statutory functions and its assessments about risk.

The project found no systemic issues, but made a number of observations in relation to specific cases reviewed and matters of best practice. These are summarised in the IGIS annual report. ASIO has advised it will consider those observations to ensure it meets best practice.

ASIO requests for information from Intelligence Services Act agencies

During the reporting period we finalised an inspection project to review ASIO requests for information (RFIs) to agencies governed by the *Intelligence Services Act 2001* (ISA). The purpose of the project was to provide assurance that ISA agencies were being appropriately informed when requests for information from ASIO related to an Australian person.

The review observed that ASD had a robust system for receiving, processing and disseminating RFIs from external agencies, but both ASIO and ASIS lacked any form of centralised system. Despite this shortcoming, the review concluded that in most of the RFIs reviewed ASIO provided all available information required for ISA agencies to meet their obligations under the ISA. One omission was identified, but this was based on security grounds. The IGIS made some recommendations with regard to standardised processes and a mandatory field to identify whether the subject is an Australian person.

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 that intelligence *in accordance with the Government's requirements*. 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 specific 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

Subject to limited exceptions (discussed below on page 12), 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 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 information 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

During the reporting period ASIS implemented an agency-wide compliance training program. The program focuses on compliance with ASIS's legislative and internal policy framework, drawing on case studies for scenario based learning. Training is compulsory for all ASIS officers, whether based in Australia or overseas. This training is regularly updated to incorporate lessons learnt from IGIS reviews and inquiries.

Ministerial authorisations

There were three cases where IGIS undertook further investigation to establish if ASIS had taken action to produce intelligence on an Australian person without appropriate ministerial authorisations. In two of these cases ASIS conducted a review of the operation and agreed collection had taken place against two Australian persons without ministerial authorisation (one of these reviews was finalised after the reporting period). ASIS advised that specific additional training

was provided to staff in the areas where unauthorised collection occurred. In the third case no breach was found.

ASIS advised the IGIS of a breach of the obligation to inform the Minister if the grounds on which a ministerial authorisation was given cease to have effect. Our inspections identified two further occasions where there were delays in informing the Minister that the grounds on which an authorisation was issued had ceased.

Legislative changes during the reporting period allow ASIS to produce intelligence on an Australian person, or a class of Australian persons, to support ASIO in the performance of its functions, without first obtaining authorisation from the Minister for Foreign Affairs. For this new power to be enlivened either ASIO needs to give ASIS a notice saying that it requires the production of intelligence on the Australian person or class of Australian persons, or an authorised ASIS officer must reasonably believe that it is not practicable in the circumstances for ASIO to notify ASIS before the intelligence can be collected. We conducted an inspection to review requests from ASIO and did not identify any issues of concern. There were no instances where ASIS relied on an ASIS officer reasonably believing that it was not practicable in the circumstances for ASIO to notify ASIS before intelligence about an Australian could be collected.

Other legislative changes also make provision for the Minister for Foreign Affairs to authorise the production of intelligence on, or have a direct effect on, one or more members of a class of Australian persons when providing assistance to the Australian Defence Force. No such authorisations were given during the reporting period.

New provisions were also inserted in the ISA to allow approval to be given to produce intelligence on an Australian in an emergency. ASIS did not use these provisions during the reporting period.

Privacy rules

Throughout the reporting period there were a number of occasions identified where the privacy rules were not applied to reporting on an Australian person or company due either to human or to technical error. Some of these occasions were identified during IGIS inspections, others were reported by ASIS. ASIS has acknowledged that the errors were due to a combination of a lack of understanding of the correct procedures by staff, unclear policies and the effect of an ageing IT system. The number of cases where there were issues was a very small percentage of the overall amount of intelligence activity undertaken by ASIS.

Cooperation with foreign liaisons

In October 2014 ASIS advised that information had been communicated to a foreign liaison without the application of the privacy rules and without approval under ASIS internal policy. ASIS advised the communication of this information was also a breach of section 9 of the ISA, which requires ministerial authorisation to undertake an activity that will or is likely to have a direct effect on an Australian person.

In March 2015 ASIS provided a summary of seven occasions where intelligence information had been provided to foreign liaisons without the application of the privacy rules and without approval under the ASIS internal policy. One of the cases was originally identified through an IGIS inspection

in February 2015 and the other cases were mostly self-reported by ASIS following raised awareness of the issue as a result of ASIS compliance training.

At a subsequent inspection in April 2015, IGIS staff identified a number of additional cases where intelligence information had been provided to foreign liaisons without the application of the privacy rules and internal approval. ASIS advised that a lack of awareness by staff of the breadth of the definition of 'intelligence information' for the purpose of the privacy rules was a significant contributing factor.

In June 2015 ASIS advised IGIS that they had cooperated with a foreign liaison service prior to obtaining ministerial approval to do so contrary to section 13(1)(c) of the ISA and internal ASIS policy. An ASIS review of the incident was conducted in April 2015. The review resulted in a number of recommendations, including reinforcing ASIS policy on the legislative requirement for cooperation with foreign authorities.

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.

The sensitive nature of ASIS's operational activities means specific detail about certain issues arising from these inspections cannot be disclosed in a public report. It was noted that internal approvals for operational activities were not always apparent on the relevant files. While in some cases there were acceptable explanations for approvals not being documented, ASIS was reminded of the importance of official records containing a complete and accurate record of approvals. This issue is being addressed by ASIS, including through the agency-wide compliance training program.

Authorisations relating to the use of weapons

ASIS met reporting requirements under the ISA in relation to use of weapons during 2014–15 and the IGIS was satisfied that there is a genuine need for limited numbers of ASIS staff to have access to weapons for self-defence in order to perform their duties.

During the 2014 Weapons Inquiry an occasion was identified where ASIS staff had participated in weapons familiarisation in controlled conditions under ADF supervision without the required prior approval by the Minister to fire the weapons concerned. It became apparent that ASIS staff did not realise this was a breach of the ISA, which suggested a deficiency in ASIS training for staff about the legislative requirements. At our request, ASIS provided a report of all other occasions where a similar breach of the ISA had occurred. A very significant number of ASIS officers had fired weapons without authorisation, either once or on several occasions. This indicated a widespread lack of understanding about the legal requirements, however, in all cases the weapons were fired in a controlled environment under qualified ADF supervision. Changes made to the ISA during the reporting period mean that in future such activities will not constitute a breach of the ISA.

We conducted two inspections of ASIS weapons and self-defence training records in 2014–15. The inspections found that ASIS's current governance and recordkeeping on this matter were effective, with no new breaches of the ISA or non-compliance with the ASIS internal weapons guidelines noted during the reporting period.

While reviewing files as a part of an IGIS Act investigation into a complaint, we identified a further breach of the ASIS weapons guidelines that had occurred a number of years earlier. In that case appropriate internal approval had not been obtained prior to an external training provider being engaged. Although the training provider met the necessary competency standards to provide specialist training of the kind ASIS required, ASIS acknowledged that under the guidelines the provision of this training should not have occurred without internal approval having first been obtained.

Inspection of ASD activities

In addition to the inquiry relating to ASD activities conducted during this reporting period, routine IGIS inspections of ASD activities for compliance with the ISA and internal policies and procedures continued. The inspections included OIGIS staff directly accessing relevant classified databases and reviewing relevant hardcopy documentation. Inspections of ASD had a particular focus on the potential impact of ASD's intelligence collection on the privacy of Australians.

Ministerial authorisations

During 2014-15 a number of ministerial authorisations which were identified for renewal lapsed for a period of time before being renewed. Because ASD and AGO make joint submissions, in most cases both agencies were affected. Administration for the authorisations is managed by ASD. In most cases, it appears the issue was caused by the delayed receipt of information required from another agency and finalising the submission for the Minister. The scale of this issue became apparent late in the reporting period, and will continue to be reviewed by this office.

ASD advised of one incident where a ministerial authorisation to collect intelligence on an Australian person expired but activities did not cease until nine days later. No information was collected or reported during that time.

ASD also advised IGIS of four occasions they had failed to report to the Minister activities conducted under a ministerial authorisation within three months of it ceasing.

In late 2014 the circumstances relevant to an activity conducted under a ministerial authorisation changed in a material way without ASD becoming aware of that change until after its occurrence. Once alerted to these changed circumstances (which were beyond the control of ASD), immediate and appropriate steps were taken to cease the activity.

During the reporting period a ministerial authorisation was given to ASD to support a specified activity conducted by the Australian Defence Force. An extended period of time elapsed between the cessation of the Australian Defence Force activity and ASD actions to cancel the ministerial authorisation and provide a report to the minister. ASD advised that this was due to uncertainty as to whether further assistance may be required.

Emergency ministerial authorisations

In the first half of the reporting period a situation arose where ASD were advised of a significant emergent threat out of hours and a ministerial authorisation for ASD to collect intelligence in relation to an identified Australian person was given orally by the Minister for Defence. At the time this decision was made, the ISA allowed for the Attorney-General to provide agreement orally in relation to a threat to security and allowed for certain other ministers to give a ministerial

authorisation in writing where the minister responsible for the agency was not reasonably contactable or available. However, the ISA did not at that time provide for the ministerial authorisation itself to be given orally. In this instance the decision was followed up by a written authorisation in the standard format within twenty four hours. Legislative amendments have now been made to address the practical issues that this situation highlighted, allowing for emergency ministerial authorisations to be given orally by ministers and, in extremely limited circumstances, by agency heads.

A small number of emergency ministerial authorisations have been given to ASD since the legislation was enacted. On each occasion the IGIS was notified promptly and the formal reporting requirements set out in the ISA were complied with. The IGIS was satisfied with the records produced in relation to each event. In two cases an issue was identified with the way that the subject of the authorisation was described but it was clear the minister intended to authorise the proposed operation.

The new provisions allowing an agency head to give an authorisation in an emergency when the minister is not available were not used by ASD during the reporting period.

Privacy rules

Two instances were identified where ASD incorrectly applied the presumption of nationality resulting in a breach of the privacy rules. In both cases information indicating that the individuals were Australian was available within ASD at the time nationality was assessed but this information was not sufficiently communicated and considered. There was no intelligence collection against Australian persons under the incorrect presumption of nationality. In one case internal ASD processes and procedures were sufficient to identify and rectify the issue in less than thirty six hours. The other case was identified and remedied in nine days.

ASD undertook an internal review of these cases and has proposed follow up actions including the revision of internal policy.

ASD also reported to IGIS on a number of occasions where a presumption of nationality had been made, and was reasonable at the time it was made, but was later overturned by new information. These cases were managed consistently with the privacy rules. The ASD processes in place for reporting to IGIS and informing other intelligence agencies when a presumption of nationality is overturned are sound.

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

At the end of the reporting period there were a small number of internal ASD compliance investigations still ongoing, including two possible breaches of the TIA Act. We continue to monitor these matters.

Inspection of AGO activities

During 2014–15 we conducted three inspection visits to AGO headquarters, as well as reviewing records of some of its intelligence collection activities on-line and discussing relevant matters with the Director of AGO and relevant officers.

The Director of AGO is required to personally authorise any intelligence collection activity undertaken by AGO in relation to Australian territory. These approvals are reported to the minister

on a quarterly basis. OIGIS staff reviewed approximately 70% of the approvals given by the Director of AGO and subsequent post-activity reports in 2014–15. No issues of concern were identified.

OIGIS staff also examined the adequacy of checks undertaken by AGO to determine the nationality of individuals or entities before targeted collection activities took place (to establish whether or not a ministerial authorisation needed to be obtained), and the extent of cooperation between AGO and other intelligence collection agencies when seeking to obtain intelligence information about the same target, or lodge a submission to obtain a joint ministerial authorisation. The only significant issue was that on a number of occasions joint ASD-AGO submissions to the minister to renew authorisations do not appear to have been processed in time; as discussed above ASD is the lead agency for administration of these arrangements.

AGO advised this office of one occasion where incomplete information about activities conducted in reliance on a ministerial authorisation was provided to their Minister. We are satisfied that the remedial actions AGO took to correct the information provided and to inform this office of the issue were satisfactory.

Based on these inspection and review activities, the IGIS was satisfied that AGO takes its statutory obligations under the ISA seriously and has put in place robust systems to encourage compliance with its obligations. AGO has effective mechanisms for identifying legal issues and ensuring that legal advice is appropriately recorded and potential issues brought to the attention of the Director of AGO.

Monitoring DIO and ONA

As has been the practice of this office over many years, we continued to exercise a light touch inspection regime with respect to the activities of ONA and DIO. As these agencies do not directly 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 the compliance of ONA and DIO with their respective privacy guidelines at least twice a year. In 2014–15 we undertook three such inspections of DIO, and two of ONA.

These inspections revealed that ONA and DIO are generally compliant with the requirements of their privacy guidelines and that they take their privacy responsibilities seriously. To the extent that non-compliance issues were identified these tended to be administrative in nature and there was no evidence that intelligence was passed in breach of the guidelines.

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 for the purpose of carrying out their functions.

The legislation also imposes reporting, administration and audit regimes on those agencies using assumed identities. This includes a requirement for ASIO and ASIS 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. During 2014-15, the Director-General of Security and the Director-General of ASIS provided the IGIS with reports covering the activities of

their respective agencies for the previous reporting period (2013-14). There was nothing in the reports that caused concern.

ASIS provided the IGIS with a copy of their internal audit reporting on assumed identities during this reporting period in addition to the annual report. This was in response to our request for this information following an inspection of ASIS assumed identity records conducted during the previous reporting period.

Light cover

Light cover is used by ASIO and ASIS staff to conceal their employment. Where more robust cover is required the agencies are able to use the assumed identities scheme (see above). In 2014, the IGIS conducted an inspection project on the agencies' use of light cover, focusing on advice, training and support provided to staff. The project identified four key areas of potential concern for staff using light cover: risk of penalties for impersonating a Commonwealth Officer when using alternative government departments as light cover; court appearances; dealing with police; and obtaining private insurance policies. Both agencies were aware of the issues, but the communication to staff in the form of policy, intranet advice and training varied. Since the completion of this project, ASIO has finalised a light cover policy. ASIO and ASIS have also sought to identify suitable life insurance options for their staff.

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 a memorandum of understanding (MOU) with AUSTRAC. This MOU establishes an agreed understanding of IGIS's role in monitoring agencies' access to, and use of, AUSTRAC information.

During 2014–15, in accordance with the MOU, the IGIS sent an annual statement to the Attorney-General and the Minister for Foreign Affairs on the outcome of compliance monitoring activities in ASIO and ASIS respectively, concerning their access to, and use of, AUSTRAC information in the previous reporting period. AUSTRAC provided insufficient information for compliance monitoring activities to be carried out in relation to AGO, ASD, DIO and ONA concerning their access to, and use of AUSTRAC information in the 2013–14 reporting period. This issue has been raised with AUSTRAC and the flow of information for this reporting period has improved and will be reported on in the 2015–16 IGIS annual report.

ASIO

Regular inspections of ASIO's access to AUSTRAC material identified the following:

- an ongoing issue with inconsistency between two of ASIO's internal policies relating to setting limitations for searches of AUSTRAC databases. ASIO have advised that there are changes to AUSTRAC databases and policies to be implemented in the next reporting period;

- two cases were identified where requests for AUSTRAC data were not authorised prior to the search being conducted. Another request was not authorised by an ASIO officer at the correct level as required by ASIO policies;
- one search of the AUSTRAC database was conducted on a partial number and returned a large number of records unconnected to the subject of the AUSTRAC request. ASIO advised that these records were not viewed by ASIO staff.

ASIS

Inspections throughout 2014–15 did not identify any significant concerns relating to the receipt of AUSTRAC material. This is a substantial improvement on previous years. ASIS has recently re-established direct access to AUSTRAC databases and information and our inspection activities are being expanded to cover this development.

Also during the reporting period ASIS advised that the AUSTRAC CEO had provided ASIS with an exemption from sections 53, 55 and 59 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* dated 16 April 2015. Essentially, this exempts ASIS from reporting movements of physical currency and bearer negotiable instruments into or out of Australia, when carrying out a statutory function under section 6 of the *Intelligence Services Act 2001*. This was in response to issues identified by the IGIS, as noted in our previous annual report.

Complaints to the IGIS office

The IGIS office receives complaints from members of the public as well as current and former Commonwealth officials. We consider a matter to be a 'complaint' if it concerns a credible allegation about illegality or impropriety in relation to an action of an intelligence agency. Complaints can be made orally or in writing.

In 2014–15, IGIS received a total of 496 complaints, of which 473 were about delay with visa-related security assessments and 23 were non visa-related. The number of visa-related complaints has remained fairly stable. The number of non-visa complaints has increased somewhat but the number still remains relatively low. Of the non-visa complaints, nineteen were about ASIO, while three related to ASIS and one to ASD.

Visa security assessments

As in previous years, complaints about visa security assessments came from a wide variety of individuals, with the largest number of complaints coming from individuals seeking skilled business or work visas (64%). There were also a substantial number of complaints in relation to family reunion visas (18%) and protection or refugee visas (16%).

The main complaint about visa security assessments is delay. Most of the factors that lead to these delays are outside of ASIO's control.

The visa complaints inspections identified a small number of issues. In each case ASIO took action to rectify the issue.

- In one case an inspection found that ASIO had not given advice to Immigration about a particular visa case even though ASIO's assessment had been completed.
- Another issue related to ensuring that cases are administratively 'unassigned' when a staff member who had been assigned the case leaves the area or ceases working on the case for some other reason. If cases are not 'unassigned' appropriately they cannot be 'reassigned' to another staff member and this can lead to unnecessary delays.

During the reporting period we received a small number of complaints from individuals who had received adverse security assessments (ASAs) in relation to their visa applications or had their visas cancelled. These individuals were all in immigration detention. OIGIS staff examined procedural aspects of the ASAs made by ASIO. In one case, the person's protection claims had not been processed so they were not eligible for a review by the Independent Reviewer of Adverse Security Assessments. The Inspector-General decided to review the person's ASA. Following the review, the Inspector-General suggested that ASIO review its decision to issue the ASA within 18 months and consider whether any changes in circumstances would change the risk to security.

Non-visa related complaints

The complaints covered a broad array of matters, including:

- concerns about the manner in which search warrants were executed and related interaction between the subjects of those warrants and ASIO;
- the basis for, and processes associated with, several sensitive individual security assessments;
- the removal of security clearances from agency employees leading to the termination of their employment;
- members of the public making credible claims of detriment caused by the actions of intelligence agencies;
- the potential impact of organisational suitability testing results on private sector employment opportunities;
- the effectiveness or otherwise of IT security arrangements to protect personal information contained in on-line job applications from prospective employees;
- delays in Aviation Security Identification Card (ASIC) and Maritime Security Identification Card (MSIC) security checks.

Public Interest Disclosure Scheme

The Public Interest Disclosure (PID) scheme commenced on 15 January 2014. In the reporting period four disclosures were made to IGIS under the PID scheme.

- One disclosure was made by a former employee of an intelligence agency who raised concerns about the legality and propriety of operational activities allegedly undertaken by an Australian intelligence agency in cooperation with a foreign intelligence agency in Australia a number of years earlier at a specific location. Following investigation, the Inspector-General found no evidence to substantiate claims that conduct of the kind alleged by the discloser had in fact occurred. The investigation identified another matter, not raised in the original complaint, which was pursued separately with the agency.

- The second disclosure was made by an individual who previously had a close working relationship with one of the intelligence agencies and was deemed to be a 'public official' for the purposes of the PID Act. This matter included a contractual dispute and also raised broader concerns about agency conduct which fell within the ambit of the PID Act. The IGIS found that there were serious gaps in the record keeping of the relevant agency which impeded the IGIS investigation and that in light of the seriousness of some of the concerns, better systems should have been in place to ensure these were detected and addressed earlier.
- The third disclosure involved claims of workplace bullying and harassment which were allegedly left unaddressed by management. This matter was allocated to the relevant agency, with the investigation report being provided to the IGIS at its conclusion.
- The fourth disclosure raised issues which had previously been the subject of thorough review, and the new issues raised in the disclosure were found not to meet the PID threshold.

In addition to the four disclosures made directly to the Inspector-General the intelligence agencies advised this office that four PID cases had been processed by the agencies during the reporting period.

The year ahead

Dr Vivienne Thom's term as IGIS ended shortly after the end of the reporting period, and the Government appointed the Hon Margaret Stone as IGIS for a five year term from 24 August 2015. During 2015-16 the IGIS will continue to focus on those areas of recent legislative amendment as well as continued focus on higher risk and more intrusive activities of the agencies. The ASD inquiry was close to finalisation at the end of the 2014-15 reporting period, and over the 2015-16 reporting period the IGIS will monitor implementation of recommendations from the ASD Inquiry as well as implementation by ASIS of recommendations from the 2014 Weapons Inquiry.