Review of Administration and Expenditure No.15 (2015-2016)

Submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone
Inspector-General of Intelligence and Security

8 December 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 2015-16 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. Office staff have access to all documents of the intelligence agencies and the IGIS is often proactively briefed about sensitive operations.

In the previous reporting period the Government announced that the office would be exempt from the efficiency dividend from 2015-16. The office also received additional funding in recent years in light of expanded oversight responsibilities flowing from legislative changes. The exemption and extra funding allowed for the recruitment of additional staff to help the office continue its comprehensive and effective oversight program. Despite a range of recruitment and selection processes during the reporting period, staff turnover and lengthy security clearance processes before new staff can be appointed have challenged our attempts to increase staffing levels. On the positive side, we do now have a dedicated corporate officer to undertake tasks such as finance and human resource management, and this has relieved investigative staff of these duties. New recruitment processes are also ongoing.

The budget funding for the IGIS office for 2015-16 was $3.05 million, and the budget for 2016-17 is $3.118 million. At 30 June 2016 the IGIS was supported by 14 staff, a number of whom were part-time.

Details of the activities of the IGIS office are set out in the 2015-16 IGIS annual report, available on the IGIS website. This submission highlights relevant issues for the Committee.

Summary

After significant legislative change during the previous reporting period, 2015-16 has been a time of consolidation in our inspection work. The national security legislative reforms enacted over the past two years substantially increased the powers of the intelligence agencies and our oversight responsibilities. The changes required a revision of our work program and existing inspection methodology to focus on the use of the new powers and higher risk activities.

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 IGIS oversight in 2015-16 include:

- An inquiry into certain actions of ASD was finalised during the early part of the reporting period.

- We continued our program of regular inspection of agency records. During 2015-16, particular focus continued to be given to inspection of the agencies' use of new and amended powers, such as special intelligence operations, identified person warrants and emergency authorisations. While the majority of inspections found no issues of concern, when issues were found they resulted in further scrutiny and we observed changes to agency practices in order to prevent reoccurrence. As with previous years, inspection activities were given priority on a risk management approach, within the resources available to us.

- We handled numerous complaints during 2015-16, however there was an overall decline in the number of complaints, compared to previous years, due to a decrease in the number of visa-related complaints. There was a slight increase in the number of other complaints and contacts with our office. There were also four Public Interest Disclosures handled by our office in 2015-16, the same number as for the previous year. Although a majority of the complaints were resolved without identifying significant issues, there were a number which raised credible concerns which were also able to be resolved.

- No new matters arising from inspections or complaints were considered by the Inspector-General to warrant investigation by means of a formal inquiry, and there were also no matters referred to the IGIS by a minister for inquiry.

- Overall the level of compliance in each of the intelligence agencies continued to be very high. While IGIS inspections and projects 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 2015-16 the IGIS completed an inquiry into certain actions of ASD. The inquiry was initiated in February 2015 by the then IGIS pursuant to s.8(2) of the IGIS Act. The final report was provided to ASD in July 2015.

The report included four (classified) recommendations, however it did not find any failure of ASD to comply with the law, nor did it reveal any systemic failures of governance or improper activity. As requested, ASD responded to the report in October 2015.

ASD accepted the principles underlying the recommendations and the Inspector-General was satisfied that ASD has appropriate ongoing arrangements in place in relation to the subject of the inquiry and was responsive to the recommendations. Routine reporting arrangements between ASD and the office have been revised to ensure appropriate levels of ongoing oversight in relation to the subject of the inquiry.

No new inquiries were commenced in 2015-16. This was mainly due to there being no major issue of concern arising during the period, a decision to prioritise the inspection of new functions carried out by agencies as a result of legislative change, there being no referrals received from a responsible minister and no substantiated complaint of sufficient complexity or seriousness to warrant an inquiry.

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 issues were identified in our annual report are noted below. Information on other inspection activities is provided in the 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 inspections of ASIO records in 2015-16 included inspection of:

- investigative cases
- human source management
- warrants
- special intelligence operations
- access to telecommunications data
- exchange of information with Australian government agencies
- exchange of information with foreign liaisons
- submissions to the Attorney-General
- security assessments

We also commenced new areas of inspection during 2015-16 in order to ensure that there was no gap in our oversight of certain types of inquiry and investigations. This included a new inspection focused on analytical tradecraft.

Investigative cases

Our inspections focused on areas where authorisation and delegation levels were lowered as part of a broad review of ASIO's internal policies and procedures, as well as on ASIO's investigative activities in relation to people under 18 years of age, noting that there is an increasing number of young people who are of interest to ASIO. There were no issues of major concern, however we will continue to focus on these areas in our inspections.

ASIO's access to prospective telecommunications data and historical telecommunications data was also reviewed as part of our regular inspection of investigative cases. In one case there was an error in a telecommunications provider's interception system which meant ASIO received unauthorised data. However, the inspections revealed that prospective data authorisations were endorsed at an appropriate level and that ASIO has regard to the Attorney-General's Guidelines and is meeting the legislative requirement to make requests for data only in the performance of its functions.

Warrants

Inspections of warrants were undertaken quarterly, as well as in the course of regular inspections of investigative cases. During the reporting period there were some breaches or errors in the execution of warrant powers. These included two breaches of the ASIO Act and seven breaches of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) relating to:

- data continuing to be collected after warrants were revoked (the warrants were revoked at ASIO's request because the circumstances under which the warrants were sought had ceased to exist)
- a carrier being advised seven days after internal approval to remove two services (rather than immediately as required by the TIA Act)
- an incorrect service being intercepted due to an incorrect telephone number being provided by ASIO.

We were satisfied these breaches arose from human error and did not evidence any systemic practice, and that ASIO took prompt remedial action to minimise the consequences as well as other action to ensure similar errors do not occur.

An area of focus during warrant inspections was the use of the relatively new identified person warrant. There were two breaches in the execution of powers under those warrants. One related to an ASIO officer acting on oral rather than written approval to exercise authority under a warrant. The other occurred after ASIO obtained the Attorney-General's conditional approval to access computers, conduct searches and use surveillance devices but due to an administrative oversight ASIO did not seek specific authorisation as the legislation required it to do, either from the Attorney-General or the Director-General of Security, prior to accessing a computer. We were satisfied that the access occurred in error, that ASIO took appropriate remedial action, and implemented adequate new measures to reduce the risk of breaches occurring.

One practical outcome from our inspections of identified person warrants was an improvement in ASIO's reporting to the Attorney-General in order to provide a better picture of how identified person warrants were being used and how they had assisted ASIO in the performance of functions.

A new type of warrant to come into effect during 2015-2016 was the journalist information warrant. We confirmed that ASIO has policies and procedures in place to address the new warrant requirements and provide staff training. We will continue to review these policies and procedures in the course of our regular inspections.

Use of force

In the previous period we reported on the notification of force being used against a person under an ASIO warrant. While the then IGIS had no concern with the circumstances in which the force was used in that instance, there were some concerns about the timeliness of the notification. ASIO acknowledged the concerns and amended its policies and procedures to require more prompt notification, and we indicated we would continue to monitor closely timeliness of notification for any future uses of force. There have been no such notifications during the current reporting period.

Special intelligence operations

The office continued to focus on special intelligence operations as another relatively new power. In one case the required notification of IGIS did not occur until 10 days after an authorisation for a special intelligence operation was granted. This was not regarded as meeting the 'as soon as practicable' legislative timeframe. ASIO promptly implemented a new procedure to address this concern. We have reviewed the documentation and been briefed on each special intelligence operation approved. While we have not identified any issues of legality or propriety, we will continue to pay close attention to ASIO's use of this power.

Exchange of information

Our inspections have covered ASIO's exchanges of information both with other Australian Government agencies and with foreign authorities. Some issues relating to levels of approval and keeping of records were raised but no major concerns were identified.

Security assessments (relating to visas, passports and welfare payments)

We continued to review a sample of cases where ASIO had recommended passport suspension, cancellation or refusal, or visa (emergency or regular) cancellations. We also reviewed cases where, in consequence of a security assessment for passport purposes, the Government may consider cancelling a person's entitlement to welfare payments. We will continue to focus on these areas in future inspections.

Analytic tradecraft

The purpose of this new inspection was to examine compliance with new policies that ASIO had implemented in response to a comprehensive review by Mr Allan Gyngell AO into the state of analytical tradecraft and practices supporting the assessment function in ASIO. Although the inspection did not identify any issues of concern and we were satisfied with ASIO's policy and training, we plan to continue this inspection in the next reporting period.

ASIO 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:

- use of information holdings within ASIO
- ASIO Telecommunications Interception System
- whole of life warrants, and
- lawyers at interview.

Use of information holdings within ASIO

The purpose of this inspection project was to review ASIO's implementation and auditing of the policy introduced in June 2014 concerning staff use of ASIO's information holdings. The policy emphasises that information holdings within ASIO are only for official purposes and not for matters which may be relevant to staff's personal circumstances (such as personal security concerns which should be raised with the relevant areas within ASIO).

In the course of the inspection project, ASIO provided us with details of guidance material and training provided to staff on the new policy and the audits conducted to determine compliance. ASIO also identified three instances of non-compliance with the policy. These instances did not raise any serious or systemic concerns but we felt that they did highlight the need for ASIO to continue its efforts to ensure that staff were aware of their responsibilities. ASIO agreed to consider other ways to remind staff of their security obligations, and to provide us with periodic updates on the results of audits and any instances of non-compliance with the policy. We will continue to monitor this issue.

ASIO Telecommunications Interception System

During the reporting period we reviewed certain telecommunications activities as part of an inspection project. A compliance issue was identified where data had not been deleted from ASIO's

systems (although it had been quarantined awaiting deletion) despite ASIO having advised the IGIS that it had been deleted. ASIO advised the error was due to a vendor system setting and subsequently rectified it. While we were satisfied that it was a simple oversight, we noted the importance of accurate advice to our office in these matters.

Warrants 'whole of life' project

During the reporting period we finalised an inspection project to review four sets of warrants where consecutive warrants have been issued over time. The purpose of the project was to review the underlying intelligence case for each warrant and to consider whether the intelligence case put to the Attorney-General each time the warrant was raised was accurate and balanced. The review concluded that ASIO generally managed the warrant renewal process with appropriate consideration of its legal obligations and consistently with ASIO's internal policies and procedures. The project found no systemic issues, but made a number of observations (which are summarised in our annual report) as well as noting improvements in source documentation between 2011 and 2014 warrants.

Lawyers at interview

During the reporting period we conducted an inspection project to follow up on an inquiry the previous IGIS had carried out in 2013. The inquiry, which concerned the attendance of legal representatives at ASIO interviews and related matters, had made five recommendations. The inspection project reviewed ASIO's implementation of the inquiry's recommendations. We found that ASIO had implemented the recommended changes and in particular we noted that ASIO's policies are now clearer, especially in relation to the presence of third parties at interviews and the voluntariness of the interviews.

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 we 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, 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 our 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 us with sufficient information upon which to decide whether appropriate remedial action has been taken, or further investigation and reporting back to our 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 our office.

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 2015-2016 we conducted a broad range of inspections of ASIS activities including examination of:

- operational files
- Ministerial authorisations to produce intelligence on Australian persons
- ASIS's compliance with the privacy rules
- emergency ministerial authorisations
- authorisations relating to the use of weapons.

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.

One area of close monitoring through the operational file inspections was the use of section 13B, a relatively new provision in the ISA. Section 13B allows ASIS to produce intelligence on an Australian person, or a class of Australian persons, in support of ASIO's performance of its functions, without first obtaining authorisation from the Minister for Foreign Affairs. For this power to be enlivened ASIO needs to give ASIS a notice saying that it requires the production of intelligence on the Australian person or class of Australian persons. Alternatively, an authorised ASIS officer must reasonably believe that it is not practicable in the circumstances for ASIO to notify ASIS before the intelligence about the Australian(s) can be collected.

An inspection project relating to the requests from ASIO 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 the intelligence about an Australian could be collected. We have continued to review the section 13B provisions throughout 2015-2016 and have incorporated it into our ongoing, regular operational file inspections.

Ministerial authorisations and compliance with Privacy rules

As identified in our 2015-2016 annual report there were some compliance issues relating to ministerial authorisations and privacy rules. Some of these were identified during our inspections, while others were reported by ASIS. These included:

- a number of occasions of not applying the Privacy Rules to reporting on an Australian person or company due to either human or technical error
- communicating information to a foreign liaison without the application of the privacy rules and without approval under ASIS internal policy.

Our inspections did not reveal any deliberate intent by ASIS staff to not apply the Privacy Rules. Rather, 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 total number of cases where there were issues relating to the privacy rules was a very small percentage of the overall amount of intelligence activity undertaken by ASIS. ASIS acknowledged the breaches and took remedial action. In addition, ASIS has been implementing 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.

Emergency ministerial authorisations

No issues were identified with ASIS's use of emergency ministerial authorisations during the reporting period. In the one instance of an emergency ministerial authorisation being issued by the Minister, ASIS notified us promptly in accordance with the reporting requirements in the ISA.

During 2015-2016 ASIS did not use the provision that allows an agency head to give an authorisation in an emergency when a relevant Minister is not available.

Authorisations relating to the use of weapons

ASIS met reporting requirements under the ISA in relation to use of weapons during 2015-2016 and we were satisfied that the need for a limited number of ASIS staff to have access to weapons for self-defence in order to perform their duties was genuine.

During the reporting period we conducted an inspection of ASIS weapons and self-defence training records. The inspection found that ASIS's governance and recordkeeping on this matter continued to be effective, and did not identify any breaches of the ISA or non-compliance with the ASIS internal weapons guidelines.

Inspection of ASD activities

During 2015-2016 we conducted a broad range of inspections at ASD, including examination of:

- ministerial authorisations to produce intelligence on Australian persons
- cancellations and non-renewals of ministerial authorisations
- selected ministerial authorisations for in-depth inspection
- ASD's compliance with the privacy rules
- Compliance incident reports.

The inspections involved our staff directly accessing relevant classified databases and reviewing 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

In the last reporting period we had noted that a number of ministerial authorisations that were identified for renewal lapsed for a period of time before being renewed. Legally, intelligence activities had to be suspended until a new authorisation was obtained. At the time of the last review, it appeared that this issue was caused by the delay in finalising the submission to the Minister while awaiting information from another agency.

We continued to monitor this issue in 2015-2016. While we noted a similar number of occurrences, we were satisfied that ASD, who also administers the ministerial authorisation process for AGO, has

appropriate policies and procedures in place to manage the ministerial authorisation renewal process. Requests for the information and documents required in support of the ministerial authorisation process are made in a timely manner and factor in reasonable timeframes for response. We noted an improvement in the information provided to the Minister in these circumstances, in line with feedback we had provided.

Ministerial authorisations – in-depth inspections

During 2015-2016 we commenced a new process of in-depth reviews on a small sample of ministerial authorisations. These in-depth reviews looked at the internal procedures of ASD teams for developing and reviewing the submissions, the detail of the supporting intelligence, and the accuracy of the information presented to the Minister.

The reviews identified a small number of issues, including reliance on one piece of reporting that was significantly older than the rest of the reporting without making this distinction clear to the Minister, a failure to make a key preliminary decision in accordance with normal procedure, and varied interpretations at the working level of how to assess whether ASD had a purpose to produce intelligence on a person. While these matters were not material to the ultimate decisions made by the Minister, they did indicate areas for improvement.

Noting the issues highlighted by these reviews, we commenced a regular inspection of ASD's preliminary decision making process in relation to ministerial authorisations. These inspections have not identified any issues of concern.

Privacy rules

There were some occasions where a presumption of nationality had been made, and which 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 incidents and breaches

During 2015-2016 ASD advised of three occasions of conducting activities to produce intelligence in relation to an Australian person without the Minister's authorisation.

- On one occasion, an error occurred in ASD's preliminary decision making process which meant that not all of the relevant information was considered.
- On another occasion, the production of intelligence in relation to an Australian person had been authorised but an activity continued for four days after the expiry of that authorisation.
- The third occasion was an historical breach identified through internal audit where a failure in ASD's record keeping resulted in the production of intelligence between 2010 and 2014 in relation to an Australian person without prior authorisation.

We were satisfied with the reporting of these matters and the remedial action taken as a result. We continue to monitor the implementation of internal recommendations in relation to these breaches.

There were also some breaches relating to the TIA Act, including:

- **Testing by unauthorised individuals**: The authorisation of testing activities in accordance with the ISA involves the authorisation of both the activity and the individuals conducting the activity. ASD conducted an internal investigation of an incident where unauthorised individuals had participated in authorised testing activity. The investigation identified that personnel involved in the testing activity were aware of the authorisation requirements and assumed that the required authorisation was in place. In response to this matter ASD decided that a dedicated officer would be appointed within the areas that conduct testing activities to oversee compliance with legislative and policy requirements.
- **Report not provided within timeframe required by TIA**: The TIA requires a report in relation to the activities conducted in accordance with an authorisation be provided to the Attorney-General within three months of the expiry of the authorisation. ASD prepared a report for the Attorney-General within the timeframe however it was not provided until two months after the deadline because of a series of administrative errors. Following internal investigation of this matter, we were satisfied with the improvements made to ASD's internal administrative arrangements, and all subsequent reports for 2015-2016 were submitted within the required timeframe.
- **Collection of intelligence in breach of the TIA**: An analytical oversight resulted in ASD collecting intelligence in breach of the TIA. We reviewed an internal investigation of the matter and were satisfied that there were no underlying systemic issues that contributed to this incident.

As with the other agencies, there were relatively few breaches in the context of the amount of ASD activity and they have not been reflective of systemic issues. In general, the ASD processes for reporting to IGIS, reviewing internal conduct and taking action to remedy breaches are sound.

Inspection of AGO activities

During 2015–2016 we conducted inspections at AGO on Director's approvals of intelligence collection activities in relation to Australian territory, ministerial authorisations to produce intelligence on Australian persons, cancellations and non-renewals of ministerial authorisations, and AGO's compliance with the privacy rules. We also visited AGO's Bendigo facility and examined the capabilities and scope of ongoing work at that site.

The Director of AGO is required personally to authorise any intelligence collection activity undertaken by AGO in relation to Australian territory. These approvals are reported to the Minister on a quarterly basis. We reviewed a significant sample of the approvals and subsequent post-activity compliance reports during the reporting period. While no issues of concern were identified, we did make some recommendations about administrative processes in relation to conditions imposed on an approval by the Director and were satisfied that AGO's subsequent actions are appropriate to address the issue.

We 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 issues are summarised in our annual report; there were no significant concerns.

Based on our inspection and review activities, we are satisfied that AGO takes its statutory obligations under the ISA seriously and has put in place robust systems to encourage compliance with its obligations.

Monitoring DIO and ONA

As has been the practice of our 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 2015–2016 we undertook two such inspections of both DIO and 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

During 2015-2016 we conducted inspections and projects which covered activities common to a number of agencies.

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 2015-2016, the Director-General of Security and the Director-General of ASIS provided us with reports covering the activities of their respective agencies for the previous reporting period (2014-2015). There was nothing in the reports that caused concern.

Cyber project

During 2015-2016 we conducted an inspection project focused on a specific intelligence operation conducted jointly by a team of ASD and ASIS personnel. The project reviewed the operation from the identification of the intelligence requirement, through to the planning, approval and conduct of the operation. We were satisfied that the operation was conducted appropriately and in accordance with the law.

A focus of our future activities will be revising our inspection activities in light of the increasing resources available to ASD in relation to cyber security. The allocation of our resources must be responsive to organisational and capability changes within the agencies.

Foreign Intelligence Collection review

We undertook a project to review a sample of completed Foreign Intelligence Collection (FIC) warrants (including warrants requested, executed and reported). The project accessed information from ASIO, ASD, ASIS and ONA. There was a recommendation about ensuring that comprehensive and up-to-date guidance is available for all staff involved in the FIC warrant process, but overall the FIC warrant process was found to be managed well and there were no substantial issues of concern.

Joint teams

We completed a project during 2015-2016 to increase our understanding of governance arrangements for joint teams and joint positions involving one or more Australian intelligence agencies. In relation to the two joint teams examined as part of this project, there were no concerns with the processes and systems in place for recording details of information exchanges. However, it is clear that each joint team is quite different and it is therefore difficult to reach any broad conclusions or draw comparisons between the governance arrangements without undertaking an extensive review of a range of joint teams. We may look further into this area in future projects or inspections.

Work Health and Safety Project

During 2015-2016 we considered how ASIO and ASIS apply section 12C of the *Work Health and Safety Act 2011* (the WHS Act). This section enables these agencies, in the course of maintaining Australia's national security, to exempt themselves from certain reporting required by the WHS Act. Our project examined records, reports, policies and guidelines relevant to the exemption. Both ASIO and ASIS have written declarations outlining circumstances in which the exemption could be applied, focusing, among other things, on exempting reporting and post-incident investigations in order to protect national security material. We found that both declarations and the accompanying policies and procedures were sound and appropriate.

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 our office are designated agencies for the purposes of the AML/CTF Act.

There is a memorandum of understanding (MOU) between IGIS and AUSTRAC which outlines an agreed understanding of our role in monitoring agencies' access to, and use of, AUSTRAC information.

In overseeing 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 focussed, and information passed to both Australian agencies and foreign intelligence counterparts is correctly authorised.

During 2015–2016, in accordance with the MOU, the IGIS reported to the responsible Ministers on the outcome of compliance monitoring activities in each of the agencies concerning their access to, and use of, AUSTRAC information in the previous reporting period. The results for each of the agencies are summarised in our annual report. We found only a limited number of compliance

issues. Overall the governance, record-keeping and internal training on management and use of AUSTRAC information continues to be effective.

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 2015–2016, IGIS received a total of 147 complaints. Of these, 118 were about delay with visa-related security assessments, 25 were non-visa-related, and four were public interest disclosures. The 147 complaints compares with 496 complaints in 2014-2015. This significant decline is attributable to a fall in the number of visa-related security assessment complaints from 473 (in 2014-2015) to 118 (in 2015-2016). This drop in overall complaint numbers is most likely a result of changes in national security considerations during the reporting period, and other factors for which our office is not responsible.

The number of non-visa complaints has increased slightly (from 23 in 2014-2015 to 25 in 2015-2016), but the number still remains relatively low. Of the non-visa complaints, 19 were about ASIO, four related to ASIS, one to ASD and one to DIO).

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 (49%). There were also a substantial number of complaints in relation to family visas (20%) and protection or refugee visas (21%).

The main complaint about visa security assessments is delay. Most of the factors that lead to these delays are outside of ASIO's control. Our visa complaints inspections over 2015-2016 identified a small number of issues, which were responded to appropriately.

Non-visa related complaints

The complaints covered a wide range of matters, including allegations or concerns about:

- the execution of, or legal basis for, search warrants and related interactions with ASIO
- failure to provide a duty of care to an individual who previously assisted ASIO
- discrimination and harassment based on race
- inappropriate access to information
- security assessments for passports and employment
- delays in Aviation Security Identification Card (ASIC) and Maritime Security Identification Card (MSIC) security checks.

All complainants were given advice about the action we had taken in response to their complaints. This included details about our examination of agency records and consideration of agency briefings, and our degree of confidence in the legality and propriety of agency actions. Some complainants received prompt, practical remedies as a result of their complaints. In one case, the remedy

included an apology from the agency concerned and improvements to agency systems. In another case, relating to an ASIO search warrant, ASIO attended the complainant's home and addressed the concerns personally. A further case was resolved when ASIO was able to finalise its security assessment after particularly urgent concerns were brought to its attention. Further information on complaints is contained in our annual report.

Public Interest Disclosure Scheme

During 2015-2016, four disclosures were made to the IGIS under the PID scheme.

One disclosure was made by an anonymous complainant who alleged that members of a small work unit in an Australian Intelligence Community (AIC) agency were secretly monitoring the internal communications of their workplace colleagues and using information accessed as a source of gossip and potential influence. Following investigation, a number of forensic technical checks were undertaken to identify any inappropriate conduct or unusual patterns. None were found.

The second matter was a complaint made by a serving AIC officer who had been suspended on full pay pending the formal withdrawal of the officer's security clearance and the termination of their employment. After reviewing relevant material, the IGIS identified no procedural flaws and decided that the decision of the agency head to withdraw the discloser's security clearance was not unreasonable in the circumstances.

The third disclosure revolved around claims by a former AIC agency employee that he should not have been permitted to attend specialist training in sensitive techniques relevant to his then employment, if he was already the subject of a 'review for cause' security investigation into his continued suitability to hold a security clearance. Following investigation, the IGIS was satisfied that the complainant was not actually the subject of a formal 'review for cause' process prior to the commencement of the relevant training. The IGIS found that while security related concerns had been raised about the complainant in the preceding weeks, the agency had sought to find a reasonable balance between maintaining appropriate and necessary security standards and treating the complainant in a fair and reasonable manner.

The fourth disclosure came from a former AIC agency officer who raised concerns about the manner in which a code of conduct investigation was carried out; alleged workplace bullying and harassment; and whether the agency concerned had inappropriately communicated personal information about the discloser to AIC and other agencies with a view to exclusion from future employment. The IGIS found no evidence to support the claims made by the discloser.

The year ahead

While the activities of the office will continue to be challenged by resource and recruitment constraints, in the year ahead we will maintain an approach to inspections that gives priority to the higher risk and more intrusive activities of the agencies. Possible new inquiries will also be considered for 2016-2017. Supplementing our core work, the expansion of our outreach activities and engagement with our stakeholders on matters of mutual interest will continue with the aim of raising awareness of the role of the Inspector-General and enhancing public confidence in the extensive and powerful oversight of the office.