IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Review of Administration and Expenditure 2016-2017

Submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone
Inspector-General of Intelligence and Security

30 November 2017

Table of Contents

Summary

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory officer who is responsible for reviewing the activities of Australia's six 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); and Office of National Assessments (ONA).

The overarching purpose of IGIS's activities is to provide assurance that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and acts consistently with human rights. The office directs a significant proportion of its resources towards ongoing inspection and monitoring activities, so as to identify any departure from these standards, including in the agencies' governance and control frameworks, before there is a need for major remedial action. The Inspector-General has the power to conduct an inquiry into an agency's activities, either of her own motion, at the request of the responsible Minister or in response to a complaint about an agency's activities.

While IGIS oversight is focused largely on the operational activities of the intelligence agencies, the Committee may find some of the outcomes of IGIS oversight relevant to its review of administration and expenditure. Potentially relevant points arising from IGIS oversight in 2016-17 include:

- a major inquiry into ASD during 2016-17 in which the legal issues arose from the configuration of an ASD collection system in a manner that led to ASD collecting certain telecommunications beyond the scope of the relevant warrant. There was also inadequate reporting by ASD to the Inspector-General and Ministers about the problem. When it became aware of the problem ASD promptly re-configured the system and there has been a marked improvement in ASD reporting to the Inspector-General since the commencement of the inquiry.
- an inquiry into the analytic independence of DIO which found significant improvements in DIO processes since the last such inquiry. The inquiry also found room for further improvements in recording the basis for assessments consistently.
- ASIO inspections frequently gave rise to concerns about inconsistent or inadequate record keeping and referencing as well as inadequate reporting to the Inspector-General on a breach of legislation identified by ASIO.
- a small number of compliance issues within ASIS was identified but overall the internal compliance mechanisms appear to be operating effectively.
- an inquiry into ONA's analytic independence found the agency's systems and processes to protect and promote analytic independence were appropriate and operating well.
- ASIS and each of the Defence agencies have an internal compliance unit. These units play a key role in training staff about legal and policy requirements and investigating, reporting and remediating instances of non-compliance. ASIO does not have a discrete internal compliance unit.

The Office of the Inspector-General of Intelligence and Security currently has 15 staff. With this number of staff it is very difficult to provide adequate oversight of the complex and diverse work performed by the Australian intelligence community. The Inspector-General assesses risk and allocates staff resources accordingly but current resourcing only allows for review of a small

proportion of the agencies' activities. For example during the ASD inquiry it was necessary to suspend all Defence inspections and to reduce the 'team' overseeing ASIS to one person. The recommendation in the report of the 2017 Independent Intelligence Review that the office be allocated additional resources to enable it to sustain a full-time staff of around 50 is welcome. If the Government adopts this recommendation and provides the additional resources, the Inspector-General will be able to provide much greater assurance to Ministers, the Parliament and the public that intelligence and security matters are open to scrutiny. It should, however, be noted that growth of this extent will take some time, particularly in view of the current delays in security vetting by the Australian Government Security Vetting Authority (AGSVA).

Defence Agencies

Oversight of the three Defence intelligence agencies (ASD, AGO and DIO) in 2016-17 consisted of a combination of inquiries, inspections and investigations into complaints.

Inquiry into ASD

An inquiry into certain actions of ASD found that ASD relied on incorrect legal advice in determining the parameters governing its interception of certain telecommunications. The legal framework applying to ASD is quite complex, particularly for matters examined in the inquiry. The inquiry also found inadequacies in ASD's reporting of the problem to the IGIS and to Ministers. The report included five (classified) recommendations designed to ensure that the situation would not recur and to streamline communications with the IGIS. ASD accepted all five recommendations. The details of the incorrect legal advice and relevant contextual information are classified.

During the inquiry ASD advised that factors that led to some of the problems identified arose from a lack of resources in the Legal and Compliance areas. This occurred in the context of much broader resourcing problems within ASD and at a time when there were many competing priorities facing the agency. ASD undertook to address these problems and before the end of the inquiry it had assigned additional staff to the Compliance area. Since then ASD has been addressing the problem of its legal resources.

There was a marked improvement in the openness and timeliness of ASD's reporting to IGIS during and subsequent to the inquiry. ASD also took appropriate technical measures to prevent ongoing unauthorised collection by the relevant system.

Inquiry into analytical independence of DIO

In 2016-17 the Inspector-General conducted an inquiry into the analytic independence and integrity of DIO. This was the third such inquiry in respect of DIO, with similar inquiries completed in 2008 and 2013. It was a routine inquiry, not prompted by any particular concern. The inquiry included a review of DIO policy, meetings with various staff and a detailed review of a sample DIO reports produced in a twelve months period. Like the previous DIO inquiry, the most recent inquiry critically examined elements of the report production process directed to ensuring that reports meet the required standards of independence and integrity. While the inquiry found that there is still some room for improvement in consistent recording of the basis for assessments. It noted significant improvements in DIO processes since the last such inquiry. A summary of the inquiry and recommendations is at Attachment A.

Defence inspection program

The inquiries into ASD and DIO during 2016-17 led to fewer IGIS resources being available for routine inspections. DIO inspections were limited to Privacy Rules and access to financial information; with no issues of concern being identified. Inspection of ASD and AGO activities focused on samples of:

- ministerial authorisations to produce intelligence on Australian persons;
- communications of intelligence about Australian persons under the Privacy Rules;
- cyber activities;
- access to sensitive financial information; and
- directors approvals for geospatial or imagery intelligence over Australia (AGO)

IGIS staff also reviewed compliance incident reports prepared by the ASD and AGO internal compliance areas.

The vast majority of ASD and AGO activities inspected were compliant with all legal and policy requirements; however, some areas of concern were identified either through inspections or as a result of internal review and self-reporting by the agencies. For example:

- In two separate cases the Inspector-General had concerns about the adequacy and timeliness of ASD's communications to our office. One case involved a breach of the Privacy Rules, and the other related to matters that led to the IGIS inquiry into ASD. In the case of the breach of the Privacy Rules, the Inspector-General was satisfied with the remedial actions ASD took to minimise the risk of this recurring.
- Four breaches of the *Telecommunications (Interception and Access) Act 1979* were reported by ASD and investigated by our office, three of these related to the subsequent IGIS inquiry into ASD.
- ASD reported on a breach of the *Intelligence Services Act 2001* relating to an emergency authorisation given by the Minister and made several internal recommendations to avoid future breaches. The Inspector-General concluded that the breach was more extensive than reported in ASD's investigation but that the recommendations were appropriate.
- AGO reported three breaches of the *Intelligence Services Act 2001* to our office, and in each case this office was satisfied with the remedial actions taken to prevent any future recurrence.

Complaints about the defence intelligence agencies

In 2016-17 the IGIS received a total of eight complaints and public interest disclosures about the defence intelligence agencies. The complaints and disclosures primarily concerned employment related matters including recruitment, security clearances and alleged bullying. Four cases warranted investigation by IGIS or were referred to Defence for investigation. Following these investigations Defence agreed to make changes to relevant recruitment advice, handling of certain records, advice to employees and advice to disclosers. Defence also issued a written apology to one person about an employment related matter.

Australian Security Intelligence Organisation

The IGIS inspection of ASIO activities in 2016-17 consisted of routine inspection of a sample of cases and a small number of special inspection projects. IGIS also received a number of complaints about ASIO mostly concerning delays in visa security assessments. There were no formal inquiries involving ASIO in 2016-17.

Regular inspection of investigative cases and warrants

Regular inspections of investigative cases focused on:

- the legality of ASIO's activities – including activities requiring warrants;
- the propriety of the investigative activities being proposed and undertaken;
- compliance with Ministerial guidelines including formal approval processes, the timeliness of periodic reviews and the proportionality of methods (that is, using less intrusive methods where possible and only progressing to increasingly intrusive methods as required); and
- compliance with internal policies and procedures.

Issues identified through inspections in 2016-17 included the following.

- Analytic tradecraft. This inspection followed from the IGIS inquiry in 2013 which recommended improvements in ASIO's policies, procedures and training to enable ASIO to demonstrate more clearly that its assessments are free from interference or bias. The inspection revealed ongoing inconsistencies in source referencing indicating the need for some improvement in this area. Following the inspection, ASIO implemented new analytic tradecraft policies which provide more comprehensive advice to analysts concerning referencing practices.
- Human source management. IGIS review of ASIO human source case files did not identify any issues of legality but raised concerns about some record keeping practices. This issue was discussed with senior ASIO staff and the Inspector-General accepted that the matter will be addressed.
- Visa and passport cancellations. ASIO Security assessments may lead to cancellation or refusal of visas or passports. OIGIS staff conducted two inspections reviewing security assessments that led to visa and passport cancellations. No issues of legality were identified, however the office did raise a number of issues regarding record keeping and referencing.

In 2016-17 ASIO proactively informed the IGIS of three breaches relating to warrants issued under the *Telecommunications (Interception and Access) Act 1979.* IGIS staff identified one additional breach relating to a warrant authorised under the ASIO Act. Two of the breaches were administrate in nature: one involved a report to the Attorney-General being one day late; in the other required wording was omitted from a warrant. The other two breaches involved incorrect services being intercepted: one error was attributable to AISO and the other to the carrier. IGIS staff also noted an increase in minor typographical errors in warrant documents which, though not affecting the validity of warrants, can lead to confusion. ASIO responded by implementing a mandatory peer review process for warrant documents.

ASIO has guidelines for the communication of information on Australians and foreign nationals to approved foreign authorities. These guidelines involve an internal, risk-based framework for assessing and approving the passage of information. The framework is based on such factors as ASIO's previous experience dealing with the authority, how the authority manages information, and the authority's history in relation to human rights issues. During 2016-17 a sample of foreign liaison exchanges were reviewed through the regular inspections of ASIO cases. These inspections have focussed primarily on areas of increased risk to Australian persons, such as those involved in the conflict in Syria and other high-risk areas. While no major areas of concern were identified, a small number of administrative and record keeping issues were found and have been brought to ASIO's attention. We will continue to monitor exchanges with foreign countries.

Breach of s37 of the ASIO Act

The ASIO Act requires that notice be given to subjects of an adverse or qualified security assessment. Amongst other things this notice facilitates the person's access to review rights and alerts them that they may be unable to travel. Notice of an adverse or qualified security assessment can be withheld only where the Attorney-General certifies that withholding the notice is essential to the security of the nation. Where notice is withheld the Attorney-General must reconsider giving notice at least annually. It is clear that the Attorney-General will need security advice from ASIO for this annual review to occur.

In 2016, ASIO did not provide the Attorney-General with the necessary information to enable the Attorney-General to consider whether a number of certificates should be revoked. Potentially the individuals concerned were denied the benefit of a favourable reconsideration, namely the information that their passports had been cancelled; and that the underlying security assessments could be subject to review. ASIO identified this oversight and subsequently conducted an internal review of all similar certificates. ASIO did not notify this office of the breach or subsequent review; IGIS staff became aware of the breach and the internal review while inspecting ASIO records.

ASIO's internal review identified four similarly affected cases. In each of those four cases ASIO's subsequent review resulted in ASIO changing its assessment, and recommending to the Attorney-General that withholding notice of the security assessment was no longer essential to the security of the nation. This office had some concern about the length of time taken to rectify ASIO's error; in one instance ASIO took five months to issue its advice to the Attorney-General.

The problem appears to have arisen from an administrative oversight when the provisions came into effect in December 2014. Whilst this issue has since been rectified, the Inspector-General was concerned by the significant impact of non-compliance upon the rights of the individuals. Also of concern was that ASIO had made the determination to delay notifying the Inspector-General of the problem until after it had fully resolved the matter. This decision was not in accordance with ASIO's longstanding practice of providing timely notification of non-compliance to this office. The problem was compounded by ASIO incorrectly advising the Attorney-General that it had reported the issue to the IGIS. The OIGIS identified this error through the course of its periodic inspections and ASIO subsequently wrote to the Attorney-General to correct the error. ASIO has accepted that it should notify this office immediately when issues of non-compliance are identified and has taken a number of steps to ensure that this occurs.

Complaints about ASIO

The Inspector-General received 253 complaints about security assessments for visa and citizenship applications. This is a significant increase over the 118 complaints received in the previous year. As with previous years complainants were primarily concerned about delay in assessments relating to business or work visas. We accept that ASIO has been addressing this problem and expect to see an improvement in the near future.

The IGIS received 34 other complaints about ASIO including two public interest disclosures. All of these were investigated. The complaints covered a wide range of matters, including allegations about:

- ASIO's conduct of interviews with members of the public;
- delays in returning goods seized under warrant;
- recruitment practices including discrimination on the basis of age;
- security assessments for employment;
- passport cancellation; and
- surveillance.

Examples of the result of IGIS investigations into complaints about ASIO include:

- ASIO returning items it had seized to a complainant.
- Two individuals were granted employment-related security clearances following significant periods of delay. In one of these cases ASIO identified that processing errors had led to delay in an assessment for an Aviation Security Identification Card (ASIC) and sent a written apology to the complainant. ASIO also introduced changes to some of its employment-related security assessment processing methods. These are expected to improve processing times.
- One complainant was concerned that ASIO had been involved in the confiscation overseas of a relative's Australian passport and that intervention of ASIO and another Australian agency had put the relative at risk of torture by foreign officials. Following investigation the IGIS was satisfied that the complaint was unfounded and that ASIO had not acted illegally or inappropriately. The complainant was advised of the consular assistance given to the relative an

IGIS received two public interest disclosures referring to ASIO and in each case reviewed ASIO records and received detailed briefings. Based on the information available the Inspector-General was satisfied that no further action was required.

Australian Secret Intelligence Service

The IGIS inspections of ASIS Activities in 2016-17 involved the routine inspection of Ministerial submissions and a small number of special inspection projects. IGIS officers also dealt with a number of complaints about ASIS and reviewed compliance incident reports provided by the ASIS internal compliance area. The Inspector-General received regular briefings on sensitive ASIS operations. There were no formal inquiries involving ASIS in 2016-17. Overall the level of compliance within ASIS was high. However, as a result of IGIS inspections and ASIS self-reporting several instances of non-compliance were identified in 2016-17. The issues identified included the following.

- four instances where ASIS had undertaken an activity without the authorisation required by s 8(1)(a)(i) of the *Intelligence Services Act 2001*. ASIS also conducted internal investigations into how and why the breaches occurred. While the sensitive nature of ASIS's activities means that further details of these matters cannot be provided here, the Inspector-General is satisfied that ASIS's internal investigations and subsequent remediation were methodical and thorough.
- one case where a member of ASIS engaged with a foreign Government agency without the Ministerial approval required under s 13(1)(c) of the *Intelligence Services Act 2001* . ASIS has subsequently received approval from the Minister to engage with the authority.
- two instances of minor delay in providing reports relating to emergency ministerial authorisations and one case where an emergency authorisation given by the agency head was not given in writing as required (a copy of the IGIS report into this matter was provided to the PJCIS).
- two instances of non-compliance with ASIS weapons guidelines overseas. One concerned transporting a weapon without the proper authority to do so (the weapon was secure at all times) and the other involved the unauthorised purchase of capsicum spray (the spray was not used).
- Several cases where IGIS staff were unable to locate ASIS records relating to operational files. ASIS subsequently conducted an internal investigation into the issue; it identified the source of the error as faults in its information communications technology and implemented several strategies to remedy the problem. The total number of cases involved proved to be a very small percentage of the overall volume of records produced by ASIS.

Section 13B notices

Section 13B of the *Intelligence Services Act 2001* allows ASIS to produce intelligence on an Australian person, or a class of Australian persons without first obtaining authorisation from the Minister for Foreign Affairs. For this power to be enlivened it is necessary for ASIO to provide ASIS with 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.

There are limits to the range of activities ASIS can undertake when operating under a section 13B notice, in particular ASIS cannot undertake any activity if ASIO could not undertake that activity in Australia without it being authorised by a warrant. Nevertheless, section 13B notices effectively remove the requirement for the Minister to consider personally each case involving the production of intelligence on an Australian person. The use of section 13B notices was the subject of IGIS inspections throughout 2016-17. Those inspections found that there were no instances where ASIS officers authorised collection using the section 13B power without notification from ASIO. It was also found that, as required by the legislation, an annual report was provided to the Minister and that there was no improper use of the section 13B mechanism by ASIS.

Complaints about ASIS

The office received five complaints about ASIS including two public interest disclosures. All concerned individual employment or recruitment related matters. IGIS provided advice to complainants and disclosers about the action taken and outcome of each investigation.

Office of National Assessments

In January 2017, the IGIS completed the fourth inquiry into the analytic independence of the ONA. The inquiry was not prompted by any particular concern, but was intended to update previous inquiries. As with the previous inquiries, this inquiry found no evidence of interference with the independence of ONA assessments. It made no formal recommendations.

The assessments and other documents examined indicated that ONA observes appropriate procedures. Reports reviewed contained comprehensive endnotes that captured information from both formal and informal sources. Lengthy commentary revealing the analyst's consideration of the significance of the referenced material was often included. ONA policies and practices encourage contestability, and ONA has an appropriate structure for critically reviewing key judgments made in assessments. A summary of the inquiry is at Attachment B

Attachment A – Inquiry into the analytic independence and integrity of assessments made by the Defence Intelligence Organisation

UNCLASSIFIED

IGIS
Inspector-General of
Intelligence and Security

The analytic independence and integrity of assessments made by the Defence Intelligence Organisation

Inquiry 2017

SUMMARY AND RECOMMENDATIONS

The Honourable Margaret Stone
Inspector-General of Intelligence and Security

8 September 2017

1. Summary and recommendations

1.1 The Defence Intelligence Organisation (DIO) is an all-source intelligence assessment agency within the Department of Defence. Its assessments support the functions of the Minister for Defence, the Department of Defence and the Australian Defence Force (ADF). DIO reports of its assessments play an important role in critical decision making and must reflect a high standard of analytic integrity and independence.

1.2 In November 2016 this office initiated an inquiry into the analytic independence and integrity of the assessments made by DIO. This is the third such inquiry in respect of DIO, with similar inquiries completed in 2008 and 2013. It is a routine inquiry, not prompted by any particular concern. As with the earlier inquiries, the inquiry does not address either the accuracy of DIO's assessments, or the extent to which they meet the needs of Ministers, the Department or the ADF as such issues are beyond the jurisdiction of this office. For this reason the inquiry concentrated on a review of a sample of twenty-one DIO reports of its assessments as well as a review of DIO policy and meetings with relevant DIO staff. The inquiry identified nine aspects of the report production process that contribute to the independence and integrity of DIO reports and assessments. They are:

- Initiating and scoping DIO reports
- Consultation and clearance
- Relations with other government agencies
- Training
- Language and style
- Information usage and identification of sources
- Critical review of past judgments
- DIO unpublished product
- Recordkeeping

1.3 This inquiry found no evidence of interference with the independence of DIO assessments. Generally the analytical integrity of the DIO process for producing reports is sound, though some areas for continuing improvement are highlighted in this inquiry. DIO's records of consultation and approval of draft reports have improved since the previous inquiry. Training observed during the inquiry was delivered professionally and appears to meet DIO requirements. As well DIO takes a flexible approach to meeting its analysts' needs for additional "tradecraft" training. The consistent and thorough editorial review of reports prior to publication resulted in clear language and style. The process for reviewing past judgments appears to be working well.

1.4 The review of information usage and sourcing in the sampled reports yielded mixed results. Two of the 21 sample reports did not require sourcing. Of the 19 that were considered, nine were well or excellently sourced; in six the content was not always adequately supported by the sourcing; and, in four reports there was either no referencing or they were poorly referenced. The inquiry recognises that the extent of referencing that is appropriate for a product will depend on the topic, the purpose and the timeframe within which it was produced.

1.5 The policy that governs DIO information usage and sourcing requires updating to take into account changed work practices within DIO as well as the findings of this inquiry. Since

the previous inquiry DIO has improved its recordkeeping, though there remains room to improve the maintenance of key documentation in DIO's official records management repository.

1.6 This inquiry makes the following recommendations, in addition to several other suggestions for improvement. DIO has accepted the recommendations and will report to IGIS on its progress in implementing the recommendation within six months of receiving this report. DIO is also working to address the suggestions for improvement contained in the inquiry.

Recommendation 1

DIO should continue its work to improve the quality and quantity of references included in analytical reports, and in particular should improve the consistency of endnoting and recordkeeping, by updating its endnoting and sourcing policy as soon as reasonably practicable.

Recommendation 2

DIO should ensure that its records identify the approving officer for each report, and should record that officer's status if relevant for approval. If approval requirements are changed a record should be kept of the reasons for the change.

Attachment B – Inquiry into the analytic independence of the Office of National Assessments

UNCLASSIFIED

IGIS
Inspector-General of
Intelligence and Security

Inquiry into the analytic independence of the Office of National Assessments

The Hon. Margaret Stone
Inspector-General of Intelligence and Security
under the *Inspector-General of Intelligence and Security Act 1986*

Public report

9 January 2017

1. SUMMARY

1.1 This is the fourth inquiry into the analytic independence of the Office of National Assessments (ONA) to be completed by the Inspector-General of Intelligence and Security (IGIS) since 2007. The inquiry was not prompted by a particular concern; it is intended as an update to the previous inquiries. As with previous inquiries, it did not address either the accuracy of ONA's assessments or the extent to which they meet the needs of policy officers and Ministers, such matters are beyond the jurisdiction of this office. The earlier inquiries, particularly the 2010 and 2013 inquiries, concluded that ONA had sound systems in place for developing, testing and reviewing its assessments and thus for guarding its independence. Given these earlier findings it was regarded as appropriate for the present inquiry to review a smaller sample of ONA assessments than would otherwise have been the case. Had the review of the initial sample identified any concerns additional sampling would have been undertaken however, as no such concerns arose, it was decided that additional sampling was not necessary.

1.2 The assessments and other documents examined in this inquiry indicated that within ONA appropriate procedures continue to be observed. This inquiry, as with its predecessors, found no evidence of improper interference with the independence of ONA assessments. Key factors that contributed to this finding included:

- IGIS staff were able independently to access relevant ONA records to review planning documents, records of consultation, draft assessments and the intelligence relied on to support the sampled ONA assessments.

- Draft versions of the reports that were reviewed in this inquiry contained comprehensive endnotes used to capture information from both formal and informal sources. All sampled assessment reports referenced source information which often included lengthy commentary on the significance of the referenced material reflecting the analyst's considerations and enabling comprehensive review.

- ONA policies and practices encourage contestability and there is evidence that staff regularly debate issues constructively. Differences of opinion between analysts are usually resolved by discussion and reports nuanced to reflect developed consensus. ONA has a formal dissent mechanism which, although very rarely used, provides the opportunity for an analyst to formally record their dissent and have it brought to the attention of the Director-General.

- ONA has a structured system for reviewing key judgements. These reviews are conducted periodically and indicate that ONA critically reviews the assessments it has made.

1.3 There was only one substantive change noted by this inquiry: ONA has moved to an electronic record keeping system. Like other agencies that have made this transition ONA faces the ongoing challenge of ensuring that the system is easy to use and that staff consistently save documents and emails in the correct folders so that they can be easily retrieved. It appears that a small number of analysts need additional training and encouragement to comply with record keeping requirements.

1.4 There are no formal recommendations arising from this inquiry.