



**Review of Administration and Expenditure
2017-2018**

**Submission to the Parliamentary Joint Committee
on Intelligence and Security**

The Hon Margaret Stone
Inspector-General of Intelligence and Security

10 December 2018

UNCLASSIFIED

Table of Contents

Summary	3
IGIS Approach to Role	4
Defence Agencies.....	6
Inquiry into ASD	6
Defence inspection program.....	6
Complaints about the Defence intelligence agencies.....	6
Australian Security Intelligence Organisation.....	7
ASIO inquiry	7
Regular inspection of investigative cases and warrants.....	7
Complaints about ASIO	8
Australian Secret Intelligence Service.....	10
Regular inspections.....	10
Section 13B notices.....	10
Complaints about ASIS.....	10
Office of National Assessments	11

UNCLASSIFIED

UNCLASSIFIED

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. Key relevant points arising from IGIS oversight in 2017-18 include:

- a major inquiry into ASD (commenced on 30 May 2018), which is examining reported breaches of section 7 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act), including timeliness and adequacy of reporting by ASD to my office and to the Minister for Defence.
- a major inquiry into ASIO (commenced in February 2018), pursuant to section 8(2) of the IGIS Act. The inquiry is examining the conduct and details around a multi-faceted, multi-agency foreign intelligence collection operation led by ASIO in 2017.
- ASIO inspections also frequently gave rise to concerns about inconsistent or inadequate record keeping and referencing. This meant that at times it was difficult for the office to assess compliance with legislative requirements, internal policies and procedures.
- a small number of compliance issues were identified within ASIS but overall the internal compliance mechanisms appear to be operating effectively.
- there were no substantial concerns with AGO, DIO and ONA.
- ASIS and each of the Defence agencies has 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 has a decentralised compliance framework.
- ASIS has a good system for building compliance into their operational planning and proactively engages the IGIS on high risk issues and when there are problems. The office gets a lot of comfort from the culture of compliance in ASIS. Similarly, compliance is a key focus for ASD's senior leadership and the agency is making a concerted effort to ensure compliance in a difficult technological environment. ASIO's approach to compliance is inconsistent; however, ASIO's senior leadership have committed to making improvements.

UNCLASSIFIED

UNCLASSIFIED

The Office of the Inspector-General of Intelligence and Security (the office) currently has 27 staff. The *2017 Independent Intelligence Review* recommended that the jurisdiction of the office be extended to include the intelligence functions of the Department of Home Affairs, the Australian Federal Police, the Australian Criminal Intelligence Commission, and the Australian Transaction Reports and Analysis Centre. Oversight of the intelligence functions of these four additional agencies is contingent on new legislation which is presently in its draft stage. The 2018-19 Budget allocated the funds necessary to allow the agency to grow to a full time staff of 55 to meet its expanded jurisdiction, and to move to new premises necessary to accommodate the additional staff. Expanding the size of the office to 55 by the end of 2019-20 requires significant internal resources for recruiting and training; it also depends on the completion of high level security vetting clearances for these extra staff by the Australian Government Security Vetting Agency. The move to new premises involves the construction of a very high security facility as well as upgrading information and computer technology facilities. Together these two elements amount to a very substantial task for the office to achieve by 2019-20.

IGIS Approach to Role

The 2018-2019 IGIS Corporate Plan includes the following description of how the office approaches the role of oversight.

Independent and Impartial

Independence is fundamental to the effective discharge of the Inspector-General's role. This includes independence in selecting matters for inspection or inquiry as well as in undertaking and reporting on those activities. IGIS staff have direct access to intelligence agency systems and are able to retrieve and check information independently. Our approach is impartial and our assessments unbiased.

Astute and Informed

Each of the intelligence agencies we oversee has its individual mandate; its procedures and operations are directed to that mandate. To target our inspections and inquiries effectively and efficiently we need to understand the environment in which the intelligence agencies operate as well as each agency's operational planning, risk management and approach to compliance. We also need to have a sound understanding of the techniques and technology used by the agencies to obtain, analyse and disseminate intelligence. Being well informed allows us to target our oversight efficiently and with flexibility.

Measured

We accept that in the complex environment in which intelligence agencies operate there will inevitably be errors. We encourage agencies to identify and self-report breaches and potential breaches of legislation and propriety and we assist agencies to identify errors and problems. Our focus is on identifying systemic or cultural problems in the activities of the agencies we oversee and ensuring that non-compliance with requirements of legality and propriety is as infrequent as possible in the circumstances.

Open

Much of the information that IGIS deals with is classified and cannot be released publicly. That said, we seek to include as much information as possible about our activities and our oversight of

UNCLASSIFIED

UNCLASSIFIED

intelligence agency activities in our annual report, unclassified inquiry reports and responses to complaints. We are also open about our approach to oversight. We seek to ensure that intelligence agencies provide Ministers with accurate reports of their intelligence activities; this includes reporting on their use of special powers such as warrants as well as reporting their non-compliance with legislative requirements.

Influential

Our inspections and inquiries lead to positive changes in agency processes and foster a culture of compliance. IGIS oversight is seen as a positive contribution to agency functions and a key part of the framework within which intelligence agencies operate. We work cooperatively with other oversight bodies to avoid duplication of effort. Our program of public presentations and our submissions to Parliamentary Committees encourage informed debate about the activities of the agencies as well as the policies reflected in those activities.

UNCLASSIFIED

UNCLASSIFIED

Defence Agencies

Oversight of the three Defence intelligence agencies (ASD, AGO and DIO) in 2017-18 consisted of a combination of inquiries, inspections, and investigations into complaints and public interest disclosures (PIDs).

Inquiry into ASD

The inquiry commenced on 30 May 2018 after a request was made to this office by the then Minister for Defence. The inquiry is examining reported breaches of section 7 of the TIA Act, including timeliness and adequacy of reporting by ASD to the office and to the Minister for Defence.

A draft report of the Inquiry is nearing completion; it would not be appropriate to describe the findings at this point, as these have not yet been shared with ASD. It is important to provide procedural fairness and to ensure the office has fully understood the position of the agency before forming a final view and reporting on it. The completed report will be provided to the Minister for Defence and may also be provided to other Ministers, including the Attorney-General, in accordance with the IGIS Act.

Defence inspection program

The inquiry into ASD during 2017-18 meant that fewer IGIS resources were available for other Defence-related inspections. 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;
- access to sensitive financial information; and
- Director's approvals for geospatial or imagery intelligence over Australia (specific to AGO).

IGIS staff also reviewed compliance incident reports and other incident reporting prepared by ASD and AGO internal compliance areas. These inspection activities were supplemented by briefings on various matters across the year, either requested by this office or instigated by ASD. The vast majority of ASD and AGO activities inspected were compliant with all legal and policy requirements. Some areas of concern with respect to ASD were identified through inspections, or internal review and self-reporting by ASD, particularly compliance with sections 7 and 12 of the TIA Act.

DIO inspections focused on compliance with its Privacy Guidelines, and access to sensitive financial information.

Complaints about the Defence intelligence agencies

In 2017-18 the office received a total of seven complaints and public interest disclosures in relation to the Defence intelligence agencies. The complaints and disclosures primarily concerned employment related matters including recruitment and security clearances. All cases were investigated by the office, however no evidence or illegality or impropriety was found. In one case the office established that Defence had already investigated and addressed the concerns. In others, our investigations confirmed the outcomes of Defence's own examination of concerns.

UNCLASSIFIED

UNCLASSIFIED

Australian Security Intelligence Organisation

IGIS oversight of ASIO activities in 2017-18 included two inquiries, one into ASIO and one into ASD that also examined an apparent error by ASIO in preparing warrant related instruments; inspections, and investigations into complaints. IGIS also received a number of complaints concerning delays in visa and citizenship security assessments. ASIO proactively provided an increased number of briefings to the office over the period. While deficiencies in record keeping were evident in all areas inspected in ASIO during the reporting period, ASIO has since instituted a number of measures to improve record keeping. The office will maintain a strong focus on this aspect in all future inspections to provide assurance that ASIO officers meet their record keeping obligations.

ASIO inquiry

In February 2018, the office commenced an inquiry into an ASIO matter pursuant to section 8(2) of the IGIS Act. The inquiry is ongoing and is examining the conduct and details around a multi-faceted, multi-agency foreign intelligence collection operation led by ASIO in 2017. The final report will be provided to the Minister for Home Affairs and may also be provided to other Ministers including the Attorney-General, in accordance with the IGIS Act.

Regular inspection of investigative cases and warrants

Issues identified through inspections in 2017-18 included the following:

- **Non-compliance with legislative reporting requirements:** Section 17 of the TIA Act requires ASIO to furnish the Attorney-General with a report detailing the extent to which a warrant assisted ASIO in carrying out its functions. IGIS staff identified that ASIO had provided section 17 reports to the Attorney-General prior to the expiry of warrants. Although this has been an accepted practice by ASIO in the past, the office advised ASIO that this procedure does not comply with the requirements of section 17 of the TIA Act or section 34 of the ASIO Act (which contains a similar requirement). ASIO has since amended its practices so that warrant reports are now provided to the Attorney-General after the warrant authorisation has ended.
- **Use of inappropriate warrant type:** Under the TIA Act, the Director-General of Security may request the issue of telecommunication service warrants under section 9 and named person warrants under section 9(A). In 2016, ASIO obtained a section 9 warrant for coverage of a legitimate and proper subject of ASIO attention. IGIS staff queried whether a section 9 warrant was the most appropriate warrant for this matter. This office expressed concern that the expansive interpretation adopted by ASIO of the phrase 'telecommunications service' did not accord with the narrow interpretation courts traditionally apply when considering the scope of intrusive statutory powers. ASIO agreed to replace the warrant with a named person warrant which resolved the matter.
- **Breach of section 38(7) ASIO Act:** Section 38(7) of the ASIO Act provides that ASIO's Minister must consider annually whether to revoke a certificate withholding notice of an adverse or qualified security assessment from the subject. In the 2016-17 financial year, ASIO did not provide the Attorney-General with necessary information relevant to section 38(7) of the ASIO Act on four occasions. During 2017-18, IGIS staff identified an additional case where ASIO failed to provide the Attorney-General with necessary information relevant to section 38(7) of the ASIO Act. This office also had concerns about the length of time ASIO took to rectify the errors, involving some seven months.

UNCLASSIFIED

UNCLASSIFIED

In 2017-18 ASIO proactively informed the IGIS of three breaches of section 7 of the TIA Act. In one case ASIO caused the interception of services to and from a particular communications service without warrant authorisation. This was caused by an erroneous transcription of a telephone number. ASIO have amended their practices to ensure such errors are less likely to occur. In the second case, a breakdown in internal processes led ASIO to intercept the communications of a particular telecommunications service for two months without a warrant. In the final case, data was collected on two services for 20 days in breach of a warrant condition. In each case unlawfully intercepted material was deleted.

Complaints about ASIO

The Inspector-General received 279 complaints relating to security assessments for visa and citizenship applications. This is a 10% increase over the 253 complaints received in the 2016-17 period. Unlike previous years when complainants were primarily concerned about delay in assessments relating to business or work visas, the largest number of complaints received during 2017-18 concerned citizenship applications (37% in 2017-18 compared to 5% in 2016-17).

The IGIS received 28 other complaints about ASIO including four public interest disclosures, all of which 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 technical difficulties during online testing;
- security assessments for employment;
- delay in the release of information under the *Archives Act 1983*; and
- surveillance.

The outcomes of IGIS investigations into complaints about ASIO included:

- ASIO returning items it had seized to two complainants. In one of these cases, the office noted that ASIO had offered to return items separately once they had been examined and had also offered to provide the complainant with the temporary use of similar items until the property was returned. As the complainant had declined these offers, the Inspector-General considered ASIO's offer to return all items as soon as examination was completed was not unreasonable.
- Three of the six individuals who complained about the time taken by ASIO to conduct security assessments were granted employment-related security clearances following significant periods of delay, noting that some delays were due to processing errors in agencies outside the AIC. The office is pleased with the initiatives ASIO has implemented to improve efficiency and finalise cases.

UNCLASSIFIED

UNCLASSIFIED

IGIS received four public interest disclosures relating to ASIO, all of which were investigated under the IGIS Act. In each case we reviewed ASIO records or received detailed briefings. In one matter, an ASIO staff member alleged a lack of procedural fairness during a review of their suitability to retain a Positive Vetting security clearance. While the investigation substantiated the claim that procedural fairness had not been afforded to the individual in that ASIO had not followed the procedure outlined in their written advice, IGIS staff were pleased to see that as soon as ASIO was alerted to the PID, ASIO proposed to address the problem and subsequently offered the staff member additional opportunities to provide written and oral responses to the concerns raised. ASIO initiated further investigation to inform their decision about the staff member's suitability to retain a PV clearance. We assess ASIO's remedial actions were appropriate. One case concerning an internal staffing process remains open.

UNCLASSIFIED

UNCLASSIFIED

Australian Secret Intelligence Service

The IGIS inspections of ASIS activities in 2017-18 involved the routine inspection of ministerial submissions, reviewing operational files weapons related matters and access to sensitive financial information. IGIS staff 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 2017-18.

Regular inspections

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 2017-18, including the following:

- Delays in providing some information to the Foreign Minister.
- Inconsistencies were observed in the wording of authorising instruments, which resulted in variations to the commencement date and expiry dates of the authorisations. While no compliance issues were observed, the lack of consistency increases the risk of error.
- Six compliance incident reports relating to Privacy Rules breaches.
- ASIS accessed an electronic device in Australia without informed consent from the owner of the device, in breach of section 8 of the ISA and section 25 A of the ASIO Act. ASIS informed the individual and apologised for the incident, as recommended by the Inspector-General.
- Three weapons-related incidents were occurred during the reporting period, two of which involved non-compliance with ASIS procedures and the third related to a firearms discharge.

Section 13B notices

Section 13B of the *Intelligence Services Act 2001* (ISA) 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. The use of section 13B notices was the subject of IGIS inspections throughout 2017-18. IGIS staff raised concerns about a delay in finalising internal guidance to ASIS staff on section 13B of the ISA. In response to these concerns ASIS promptly finalised internal guidance on section 13B notices.

IGIS staff also identified a delay with ASIS fulfilling its annual reporting requirement in relation to 13B notices (ASIS is required to provide an annual report to the Minister 'as soon as practicable after each year ending on 30 June'). The report for the period 2016-2017 was provided to the Minister for Foreign Affairs in January 2018. While not a breach of the ISA, the provision of the report to the Minister more than six months after the conclusion of the reporting period was not satisfactory.

Complaints about ASIS

The office received four complaints about ASIS. including two public interest disclosures. Three concerned individual employment or recruitment related matters, and one of these was considered to be premature as ASIS had offered the complainant an opportunity to express concerns which had not been taken up. The fourth matter was an anonymous disclosure concerning maladministration which contained insufficient information to be investigated and instead was considered through our inspection program. Where possible, IGIS provided advice to complainants and disclosers about the action taken and outcome of each investigation.

UNCLASSIFIED

UNCLASSIFIED

Office of National Assessments

During 2017–18, IGIS staff conducted inspections examining ONA’s compliance with its Privacy Guidelines and reviewed ONA’s policies and handling of open source information as part of a cross agency project.

ONA self-reported a small number of instances where Privacy Guidelines were not applied by ONA before publication. The office assessed that these errors did not result in the inappropriate dissemination of intelligence information about an Australian person.

UNCLASSIFIED