UNCLASSIFIED

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Review of Administration and Expenditure No. 18 (2018-2019)

Submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone AO FAAL

Inspector-General of Intelligence and Security

17 February 2020

Table of Contents

1. Introduction

The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make this submission to the Parliamentary Joint Committee on Intelligence and Security (the Committee)'s 2018–19 review of the administration and expenditure of 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 Intelligence (ONI).

Information about the role of the IGIS is at **Attachment A**.

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 matters arising from IGIS oversight in 2018-19 include:

- An inquiry identified systemic issues within ASIO's compliance management framework, which had resulted in significant problems with the planning and execution of an ASIO led multi-faceted, multi-agency foreign intelligence collection operation. The Inspector-General made eight recommendations in her report on the matter, focused on the establishment of ASIO's proposed compliance team; the implementation of an ASIO compliance training program; improving legal advice; and a review of relevant policies and procedures. ASIO has made some progress in implementing these recommendations and is working towards their full implementation.

- A separate inquiry found that unlawful interception of telecommunications by ASD had occurred as result of an error made by ASIO in preparing the relevant authorisation, and by a failure on the part of ASD to check the accuracy of the authorisation before relying on it. The inquiry found that ASD's initial reporting of this matter to the Inspector-General and the Minister for Defence was inadequate. ASD did make a comprehensive report of the matter prior to the inquiry commencing, and has improved its reporting since this incident occurred. While ASIO did not report the breaches of the warrant to the Attorney-General, ASIO has since amended its procedures and is now reporting breaches to the Attorney-General.

- An inquiry related to ASIS and ASIO stemmed from allegations made by a former ASIS officer that other ASIS officers engaged in misconduct and fraud. The inquiry found no evidence to support the allegations, either in the records reviewed or through interviews. The inquiry, however, identified areas where ASIS and ASIO could improve communication and collaboration. Four recommendations were made in the report, all of which were accepted and have now been implemented.

- There was an increase in complaints about delays in the processing of visa and citizenship applications, beyond the indicative timeframes listed on the Department of Home Affairs website. For example, some student visa applications are taking 18 months or longer to finalise.

- Most public interest disclosures received by the office concerned employment related matters, primarily concerning management actions and security clearances.

2. Australian Security Intelligence Organisation

IGIS oversight of ASIO activities in 2018-19 included three inquiries pursuant to section 8 of the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act), and inspection of ASIO's activities. One of the inquiries was into ASIO activities and the other two inquiries were into the activities of other Australian intelligence agencies with ASIO involvement. In conducting inspections, priority was given to reviewing ASIO's intelligence collection activities, security assessments and advice to Ministers on security matters. This office received 750 complaints about visa and citizenship applications. With regard to other matters, this office investigated 22 complaints against ASIO and one public interest disclosure.

2.1 ASIO inquiry

Inquiry into an ASIO matter

The IGIS submission to the 2017-18 Review of Administration and Expenditure made mention of an ongoing inquiry into an ASIO matter pursuant to section 8(2) of the IGIS Act. The inquiry examined the conduct and details concerning an ASIO led multi-faceted, multi-agency foreign intelligence collection operation, including whether certain intelligence collection activities conducted by ASIO as part of that operation were lawful. While the inquiry found significant problems with the planning and execution of the operation, stemming from systemic weaknesses within ASIO's compliance management framework, it also concluded it is likely that most, but not all, of the activities reviewed as part of the inquiry were lawful. Importantly, there was no evidence of any deliberate wrong-doing by the officers involved in the operation.

The issues identified by the inquiry included poor communication between ASIO's lawyers and operational staff. As a consequence of the poor communication ASIO staff believed, incorrectly, that a warrant was not required to undertake activities that in fact did require such authorisation. Additionally, as ASIO's lawyers were not fully informed about changes to operational plans those activities were conducted without proper advice. Other issues identified by the inquiry included failures to comply with procedural requirements for warrants and associated reports; a key secondment agreement being signed by an officer without the appropriate delegation to do so; and inadequate management and supervision of those officers ostensibly seconded to ASIO.

In addition to reviewing the circumstances surrounding the operation, the inquiry also examined ASIO's approach to compliance and training more broadly. It found that ASIO provided little if any compliance training for ASIO employees and affiliates in relation to legislative restrictions germane to the operation. The inquiry also found that whilst operational staff complied with ASIO's operational planning procedures, these procedures were inconsistent with other ASIO policies and were insufficient to ensure that ASIO acted lawfully. At the time of the incident, ASIO did not have a dedicated compliance unit; however, even before the formal recommendations outlined in the following paragraph were made, ASIO had begun to develop a formal compliance framework and to establish a dedicated compliance unit.

The final inquiry Report was issued on 14 June 2019 and made eight recommendations. The recommendations focused on the establishment of ASIO's proposed compliance team; the implementation of an ASIO compliance training program; improving legal advice; and a review of relevant policies and procedures. ASIO accepted all eight recommendations and is working towards

their full implementation. ASIO has identified milestones for the implementation of each recommendation to this office, and an inspection program has been agreed between the Inspector-General and ASIO that will see each progress towards each milestone monitored and reviewed by this office as it falls due over the next six months.

Inquiry into an ASD matter with ASIO involvement

In May 2018 this office commenced an inquiry into the unauthorised interception of telecommunications by ASD. ASD activity was facilitated by warrants sought by ASIO under the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Further detail on this inquiry is provided in section 3.1 of this submission (ASD inquiry).

Inquiry into an ASIS matter with ASIO involvement

In July 2018 this office commenced an inquiry into allegations that ASIS officers had engaged in misconduct and fraud. Further detail on this inquiry is provided in section 4.1 of this submission (ASIS inquiry).

2.2 Inspections

In 2018-19 this office conducted inspections using a variety of methodologies, including thematic reviews, risk-based sampling and random sampling. ASIO provided an increased number of proactive briefings and the overall standard of record keeping was found to have improved compared to the previous reporting period. Issues identified through inspection activity in 2018-19 included the following:

ASIO Act Warrants

This office raised two systemic issues relating to warrants under the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act). The first issue related to authorisations of classes of persons under s24 of the ASIO Act, for which this office considered some descriptions ASIO used were overly broad, uncertain or not sufficiently connected to the exercise of power under the warrant. The second issue related to the inappropriate use of templated text in briefing the Attorney-General for the purposes of s27C(2)(b) of the ASIO Act. In response to these issues, ASIO promptly amended its template.

ASIO proactively advised this office of three incidents relating to special powers under the ASIO Act. The first instance related to the unauthorised collection of information from surveillance devices under a s27F Identified Person Warrant. ASIO subsequently conducted a review of procedures with regard to warrant expiry to ensure any activities not authorised under warrant are terminated. The second instance related to mistaken access to a computer by an ASIO officer. The incident was attributable to a breakdown in internal processes. ASIO reviewed these processes with a view to preventing a recurrence. The third instance related to a search activity where a person who examined records was not authorised to do so under s24 of the ASIO Act. We are satisfied having regard to the circumstances that this is was an isolated incident that does to point to systemic weaknesses.

Interception warrants under the TIA Act

This office identified ongoing non-compliance with s17 of the TIA Act in which ASIO provided reports to the Attorney-General advising that all services named on the warrants had been intercepted

without establishing the accuracy of this advice. ASIO acknowledged the ongoing non-compliance but advised that practical difficulties rendered it impossible to completely remediate the issue in the near future. As an interim measure, ASIO has improved the accuracy of s17 reports by including explanatory notes outlining the limitations in the assurance they can provide in this regard.

ASIO proactively advised this office of a number of incidents in relation to the TIA Act including typographical errors relating to requests and warrant applications under s9A and s11B; a breach of s16 when a telecommunications carrier was not advised that ASIO had determined interception should cease; instances whereby errors made by telecommunications carriers resulted in ASIO receiving information which it was not authorised to collect; and over-collection of personal information due to delays between telecommunications carriers being advised of termination and the disconnection being effected. This office was satisfied with ASIO's response to these incidents and did not identify any propriety concerns.

Access to telecommunications data under the TIA Act

ASIO proactively advised this office of two instances relating to access to telecommunications data under the TIA Act. The first instance related to ASIO failing to revoke a s176 authorisation leading to a period where information continued to be collected. Upon identifying the non-compliance, ASIO immediately deleted the information and subsequently revised relevant processes to prevent future occurrences. The second instance involved a typographical error in a s175 authorisation resulting in ASIO collecting information relating to a telecommunications service that was not relevant to ASIO's functions. ASIO deleted the erroneously collected information within 48 hours of identifying the error.

Use of Force

This office received one notification regarding the use of force against persons during the execution of an ASIO search warrant. The force was used by law enforcement officers assisting ASIO in the execution of the warrant. The incident was subject to law enforcement internal reporting and review processes and there was no indication the force was other than reasonable and proportionate for the purpose for which it was exercised.

Special Intelligence Operations

ASIO's special intelligence operations (SIO) powers were introduced in 2014, allowing ASIO to seek authorisation from the Attorney-General to undertake activities which would otherwise be unlawful. This office identified several instances whereby SIO's were varied but participants were not formally advised in a timely manner. ASIO has subsequently revised its procedures in this regard. The office raised one propriety issue concerning the interim report for a particular SIO. The issue was addressed in the final report to the Attorney-General.

The Attorney-General's guidelines

This office identified a small number of instances whereby ASIO investigative activities were undertaken without first obtaining the proper authorisations stipulated by the Attorney-General's guidelines. However, this office assessed this was not a systemic issue. This office also noted a small number of ASIO's investigations were not reviewed within the annual limit stipulated by the guidelines. A majority of these instances were proactively reported to this office by ASIO.

ASIO proactively advised this office of two instances whereby a subject of a security investigation was subsequently determined to be not relevant to security. In both instances this office concluded that ASIO's actions were lawful and proper. This office recognised that intelligence agencies frequently work with incomplete information in environments of time pressure and on occasion conclusions require amendment as new information presents itself. This office also recognised ASIO's response in these instances was a positive demonstration of how transparency and accountability by intelligence agencies can assist in preserving the privacy of individuals.

ASIO exchange of information with foreign authorities

ASIO proactively advised this office of an incident whereby a breakdown in processes resulted in information relating to Australian citizens being disclosed to a foreign service without sufficient authorisation as per ASIO internal policy. Appropriate approval was retrospectively granted and additional procedures for foreign disclosure of information have subsequently been implemented.

Security Assessments

In a similar manner to previous years, in 2018-19 this office reviewed a number of prejudicial (adverse or qualified) security assessments. ASIO proactively advised this office of five instances where Commonwealth departments failed to furnish the required information within the time period stipulated by s38 of the ASIO Act. In all five cases, this office was satisfied that ASIO's actions were lawful and proper.

2.3 Complaints about ASIO

In 2018-19 this office received 750 complaints about visa or citizenship applications. This represents close to triple the 279 complaints received in the 2017-18 reporting period. The most frequent complaint about visa and citizenship applications remains the length of time taken to finalise an application beyond the indicative timeframes listed on the Department of Home Affairs' website. In 2018–19, the largest number of complaints related to student visas, accounting for half of all visa and citizenship-related complaints. IGIS is aware that some student visa applications are taking 18 months or longer to finalise.

The IGIS received 22 complaints about ASIO that concerned other matters, and one public interest disclosure. All were investigated. The complaints covered a wide range of matters, including allegations about:

- ASIO's conduct of interviews with members of the public
- Detriment arising from ASIO actions
- Security assessments for employment
- Recruitment practices.

The outcomes of IGIS investigations into complaints about ASIO included:

- ASIO corrected database errors and sent a letter of apology to a complainant after identifying communication failures in a recruitment process.

- ASIO amended its practice manual to include arrangements for interviewing persons with a disability in compliance with the *Disability Discrimination Act 1992*, and agreed not to interview a complainant again without an interpreter.
- Eleven of the 22 complaints about ASIO concerned delay in security assessments for security clearances required for employment in Australian Government agencies or for an Aviation Security Identity Card. ASIO information revealed that, of the 11 complaints about delay, five concerned cases that did not meet the criteria for priority assessment and had not progressed faster due to competing priorities. No concerns were identified as to the legality or propriety of any ASIO action, and this office does not interfere with the assessment itself or comment on agency resourcing decisions. Where complainants advised their work was affected by the delay, IGIS staff suggested alternative action for complainants to take, such as seeking prioritisation through their employer and the Australian Government Security Vetting Agency (AGSVA).

3. Australian Signals Directorate

IGIS oversight of ASD in 2018-19 included one inquiry pursuant to section 8 of the IGIS Act and inspections of ASD activities. The inquiry related to the unlawful interception of communications and inadequate reporting of the incident to IGIS and the Minister of Defence. In 2018-19 the IGIS received five complaints and one public interest disclosure about ASD.

3.1 ASD inquiry

In May 2018 the Inspector-General began an inquiry into the unauthorised interception of telecommunications by ASD, relating to an operation to collect communications of foreign intelligence value. The operation was facilitated by warrants sought by ASIO under the TIA Act.

In June 2017, ASD advised the Inspector-General that as a result of an error in preparing the relevant authorisation under section 12 for certain warrants, some ASD staff who were not authorised had intercepted telecommunications; in the absence of authorisation the collection was unlawful. That advice did not give any indication of the scale of the issue. By July 2017, five months after the warrants were signed, ASD staff were aware that a significant number of unlawful interceptions had occurred. This information was not conveyed to the Inspector-General or the Minister for Defence until February 2018.

The inquiry found that the unlawful interception was the result of an error made by ASIO in preparing the relevant authorisation, and by a failure on the part of ASD to check the accuracy of the authorisation before relying on it. When the error was detected ASD promptly requested a new authorisation and ASIO promptly responded to that request. ASD then undertook a lengthy internal investigation and took appropriate steps to delete all unlawful intercept.

The inquiry found that ASD's initial reporting of this matter to the Inspector-General and the Minister for Defence was inadequate. ASD did make a comprehensive report of the matter prior to the inquiry commencing, and has improved its reporting since this incident occurred. While ASIO did not report the breaches of the warrant to the Attorney-General, ASIO has since amended its procedures and is now reporting breaches to the Attorney-General.

The inquiry also found that in the past 10 years, in a relatively small percentage of the warrants that ASD was involved in executing, there had been regular legislative breaches and incidents resulting from inadequate management of warrant procedures.

The Inspector-General made five recommendations to improve the reporting of future breaches of the TIA Act, and reduce the risk of their recurrence. ASD and ASIO accepted all recommendations and have commenced implementation. ASD cooperated fully throughout the inquiry.

3.2 Inspections

During 2018-19, this office focused inspections on: applications for ministerial authorisation to produce intelligence on Australian persons; ASD's compliance with the ASD Privacy Rules; compliance incident reports; and ASD's access to sensitive financial information.

Ministerial Authorisations

The *Intelligence Services Act 2001* (ISA) requires ASD to obtain authorisation from the Minister for Defence before conducting certain activities, including the production of intelligence on Australian persons. The submissions for ministerial authorisations inspected were generally of a high standard, and no significant issues were identified. However, IGIS staff identified several instances where ASD did not display appropriate administrative restrictions on certain database records, which heightened the risk of an inadvertent breach of the ISA. ASD's response to feedback on this issue was positive and IGIS staff continue to monitor this aspect of ministerial authorisations and associated records.

Emergency Ministerial Authorisations

Situations may arise where, as a matter of urgency, ASD requires a ministerial authorisation to undertake certain activities. During the reporting period, IGIS staff reviewed three emergency ministerial authorisations issued to ASD. There were no issues of concern regarding the initial administrative management of the authorisations; however, on one occasion ASD did not provide the Minister with a section 10A report within one month of the authorisation ceasing.

Ministerial Submissions

During the reporting period IGIS staff conducted a quarterly review of ASD's submissions to the Minister for Defence. IGIS staff found that the submissions were generally of a high standard, and were provided to the Minister within an appropriate time frame. IGIS staff appreciated ASD's consultation with the IGIS office in relation to several submissions.

Protecting the privacy of Australians

The Minister for Defence issues written rules (the ASD Privacy Rules) to regulate how ASD communicates and retains intelligence information about Australian persons. In accordance with its obligations under the Privacy Rules, ASD reported on instances where ASD had initially presumed that a particular individual was not an Australian person, but where the presumption was subsequently rebutted and the person was shown to be Australian. IGIS staff reviewed these cases and found that the initial presumptions of nationality were reasonable given the information available to ASD at the time. ASD's actions, including informing other intelligence agencies that the person is Australian, were appropriate and in accordance with the Privacy Rules. The office notes that ASD, as a propriety measure, began to inform second parties of overturned presumptions of nationality in mid-2018. The office acknowledges this extra step that ASD is taking to ensure the privacy of Australian persons is protected.

Legislative non-compliance

ASD has a strong record of proactive self-reporting to the IGIS where it identifies breaches of legislation and significant or systemic matters of non-compliance with ASD policy. ASD takes mitigation and remediation actions where required in consultation with the office.

TIA Act Incident Reports

The TIA Act prohibits agencies from intercepting communications passing over a telecommunications system, except in limited circumstances, such as where there is a warrant in place allowing interception. In 2018-19, three instances of legislative non-compliance with the TIA Act occurred. In

one instance, ASD advised that it had intercepted communications without a warrant, and had then communicated the intercepted material. The office was satisfied with ASD's investigation and the remedial action taken to prevent recurrence. As of 30 June 2019, ASD confirmed a further two contraventions of the TIA Act, but had not yet completed its investigations. The office appreciates ASD's efforts to keep IGIS staff apprised of progress of investigations.

In addition to these confirmed instances of non-compliance, ASD also advises this office of 'potential breaches' where a breach is technically possible but cannot be proven. In 2018-19, two instances of potential non-compliance occurred. In October 2018, ASD advised this office of a potential breach of section 7 of the TIA Act as a result of the misconfiguration of an ASD system. This office reviewed the incident and considers that ASD potentially breached section 7 and section 63; however, the office notes that ASD acted promptly to inform the IGIS and to rectify the incident. Also in October 2018, ASD advised that it was investigating an incident in which communications were potentially intercepted due to a system error; ASD later determined the incident did not contravene legislation. This office conducted an independent review of the incident and considers that a component of the collection constituted a potential breach of section 7 of the TIA Act, as it cannot be conclusively demonstrated that the suspect interception did not occur. ASD undertook appropriate mitigation measures following both incidents.

***Intelligence Services Act 2001* Incident Reports**

In 2018-19, three instances of legislative non-compliance with the ISA occurred. In one instance, ASD conducted intelligence activities in relation to two Australian persons without obtaining authorisation from the Minister. ASD then further contravened the requirements of the ISA by conducting a subsequent activity without consideration of the ASD Privacy Rules. The second instance related to another breach of its ISA obligation to obtain a ministerial authorisation to produce intelligence on an Australian person. The third instance related to ASD's failure to provide a report to the Minister for Defence in relation to activities conducted under an emergency ministerial authorisation. This office was satisfied with ASD's investigation and remedial action to prevent recurrence in all three cases.

Other Incident Reports

In late 2018, ASD advised IGIS of an instance where it had contravened certain legislation. The sensitive nature of ASD's operational activities mean that specific details cannot be included in this report.

3.3 Complaints about ASD

In 2018-19, the IGIS received five complaints and one public interest disclosure about ASD.

Three complaints related to employment matters concerning management action or internal security. One complaint related to staff concerns arising from ASD's change to a statutory agency. No legality or propriety issues were identified in these matters.

One complaint concerned the Australian Cyber Security Centre's procedures for interacting with a member of the public who had applied for certification of encryption software and claimed to have received no response. The ACSC informed IGIS staff of their prior contact with the complainant. The person's emails had been blocked permanently due to their offensive language and threatening conduct towards ACSC staff. ASD's functions require little interaction with members of the public and the ACSC, which provides a range of services requiring public engagement, was unfamiliar with

strategies for managing such problems. IGIS staff provided advice (and relevant resources available from the Commonwealth Ombudsman) about appropriate management of unreasonable conduct. As a result, the ACSC wrote to the individual formally advising the communication restrictions, the timeframe during which the restrictions would be imposed, and conditions to be met in regard to any future contact. The ACSC expressed appreciation for the guidance IGIS staff provided and indicated an intention to incorporate it in staff training.

The public interest disclosure relating to ASD concerned maladministration resulting in the denial of a contracting position. The discloser alleged ASD did not provide procedural fairness and was concerned the denial could be reprisal action for having made a previous complaint. Investigation under the IGIS Act found no evidence to prove the allegations. While the investigation found some areas for improvement in ASD's communication and processes, these would not have changed ASD's decision in the case. The Inspector-General made two recommendations relating to ASD's internal processes and two relating to the specific case, all of which were accepted by ASD.

4. Australian Secret Intelligence Service

Overall in 2018–19, ASIS had a high level of compliance with relevant legality and policy requirements, and proactively brought to our office's attention any significant compliance concerns.

IGIS oversight of ASIS in 2018–19 included one inquiry pursuant to section 8 of the IGIS Act and a range of routine inspections of ASIS activities covering all the agency's functions. IGIS further conducted other review and oversight related activity, other than inspections and inquiries. For example, ASIS consulted the office on the legality and propriety of certain proposals and draft internal policies, to allow IGIS to identify any concerns before finalisation. To supplement inspection and oversight activities, regular bi-monthly meetings between the Inspector-General and senior ASIS staff took place to discuss different matters, and during the 2018-19 period the Inspector-General also presented to ASIS senior staff.

IGIS staff dealt with two complaints about ASIS, three public interest disclosures and one formal inquiry. The main inspection activities relating to ASIS in the 2018–19 period were the review of operational files and ministerial submissions. Other inspection activities included access to sensitive financial information, and authorisations relating to the use of weapons and reporting of compliance matters.

4.1 ASIS inquiry

There was one inquiry into ASIS, which was completed on 20 December 2018. This inquiry was led by Mr Bruce Miller AO, and the Inspector-General delegated to Mr Miller the functions and powers for him to lead the inquiry.

This inquiry stemmed from allegations made by a former ASIS officer that other ASIS officers engaged in misconduct and fraud. The inquiry found no evidence to support the allegations, either in the records reviewed or through interviews. The inquiry, however, identified areas where ASIS and ASIO could improve communication and collaboration. Four recommendations were made in the report, all of which were accepted and have now been implemented.

4.2 Inspections

Operational file inspections primarily involve reviewing ASIS records relating to the management of agents, the conduct of operations, and the running of overseas stations. Ministerial submission inspections mostly involved reviewing records of ministerial authorisations to produce intelligence on Australian persons. The following provides an unclassified overview of these and other key ASIS inspection and oversight activities by this office:

Operational files

During the 2018-19 period, this office reviewed files relating to ASIS's operational activities in a number of countries. These inspections typically focused on records created in the previous two years for a given station, source or operation. Additionally, during this period, OIGIS staff conducted a historical review of ASIS files relating to allegations of improper conduct by ASIS that occurred over ten years ago. That inspection did not identify any legality or propriety concerns.

The sensitive nature of ASIS's operational activities means that the specific detail of the topics inspected and matters identified cannot be provided in a public report. Based on records reviewed IGIS staff were satisfied with the legality and propriety of ASIS operational activities, and that ASIS officers were identifying and managing risk associated with activities in a reasonable manner.

Ministerial Submissions and Authorisations

During the 2018-19 period, IGIS staff reviewed all ministerial submissions provided by ASIS to the Minister for Foreign Affairs as part of routine inspection activity. IGIS staff were satisfied that the information provided to the Minister was appropriate. There were three cases where ASIS did not report to the Minister for Foreign Affairs within three months of the day on which a ministerial authorisation ceased to have effect as required under section 10A(2) of the ISA. IGIS inspections also identified a number of authorisations that were compliant with the ISA, but non-compliant with ASIS's own internal procedures. ASIS undertook to remind relevant staff of this requirement and the office was satisfied with this response, and will continue to review.

Section 15(5) and Privacy Rules

On 28 March 2019, the Minister for Foreign Affairs signed ASIS's new Privacy Rules which took effect on 9 May 2019. During the 2018-19 period, ASIS self-reported nine instances related to the non-application of the Privacy Rules. A further two instances of ASIS's non-application of the Privacy Rules were identified by this office. These cases were not in accordance with section 15(5) of the ISA. All cases were due to a combination of human error and issues associated with ageing IT systems. This office found no instances where reporting on an Australian person would not have been reasonable and proper, had the Privacy Rules been applied at the same time.

Authorisations relating to the use of weapons

The IGIS continues to be 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 is genuine. There were no instances of non-compliance with internal weapons guidelines issued by the Director-General of ASIS identified by ASIS or IGIS staff during the 2018-19 period. IGIS staff also examined ASIS weapons and self-defence policies, guidelines and training records during an inspection, and did not identify any issues of concern.

4.3 Complaints about ASIS

In 2018-19, the IGIS received two complaints and three public interest disclosures about ASIS.

Investigation of one complaint, which concerned a workplace injury, identified no illegality or impropriety in ASIS's handling of the case.

The second complaint alleged a law may have been breached by ASIS in the course of their work. The IGIS provided her views to the complainants and no further action was taken.

Public interest disclosures about ASIS

Three public interest disclosures concerned alleged maladministration in the conduct of security clearances for staff. No illegality or impropriety was identified in ASIS's handling of each case.

5. Office of National Intelligence

During the 2018-19 period this office had oversight of the Office of National Assessments (ONA), which became the Office of National Intelligence (ONI) on 20 December 2018 following the *Office of National Intelligence Act 2018*. In December 2018, the Prime Minister signed the ONI Privacy Rules, in accordance with section 53(6) of the ONI Act. This office was consulted extensively in the preparation of the Rules and the IGIS is satisfied that the Rules protect the privacy of Australian persons. The IGIS provided a brief to the PJCIS on the content and effect of the Rules.

The former ONA had three broad statutory functions, whereas ONI has 11 primary functions under the ONI Act. Not all of ONI's functions were a focus for this office during the reporting period. IGIS staff focused on the areas considered to be of highest compliance risk, namely the implementation of the new ONI Privacy Rules and associated policies and guidelines. This office will continue to review its approach to ONI inspections and review activity.

In 2018-19, the IGIS received no complaints or public interest disclosures about ONI.

5.1 Inspections

The functions of ONI mean it is less likely to intrude into the privacy of Australian persons or operate in breach of legislation than intelligence collection agencies. Therefore the IGIS office conducts fewer inspections of ONI than such collection agencies. The main inspection conducted was of ONI's compliance with its Privacy Rules (formerly ONA's compliance with its Privacy Guidelines). The office also inspected ONA and ONI's access to sensitive financial information.

ONI Privacy Rules

During the 2018-19 period, IGIS staff conducted one inspection and did not identify any non-compliance of ONI's Privacy Rules. It was noted that the majority of ONI's records reviewed were of a high standard, although the inspection did identify some minor areas where compliance with ONI policy could be improved

6. Australian Geospatial-Intelligence Organisation

IGIS oversight of AGO in 2018-19 included inspections of AGO activities. The IGIS received no complaints or public interest disclosures about AGO.

6.1 Inspections

During 2018-19, this office focused inspections on: applications for ministerial authorisation to produce intelligence on Australian persons; Director's approvals and post-activity reporting; AGO's compliance with the AGO Privacy Rules; and AGO's access to sensitive financial information.

Ministerial Authorisations

The ISA requires AGO to obtain authorisation from the Minister for Defence before conducting certain activities, including the production of intelligence on an Australian person. This authorisation is usually requested in conjunction with ASD. During 2018-19, IGIS reviewed all applications made by AGO for ministerial authorisation. IGIS inspections did not identify any concerns relating to AGO's applications for ministerial authorisation, renewals, or circumstances in which AGO sought to cancel an authorisation. One emergency ministerial authorisation was issued to AGO during the reporting period; IGIS staff reviewed this emergency authorisation and did not identify any issues of concern.

Director's Approvals and Post Activity Reporting

The Minister for Defence requires the Director of AGO to approve AGO activities intended to produce geospatial or imagery intelligence on a person or body corporate in Australian territory or subject to Australian jurisdiction, unless the activity is one for which AGO must seek ministerial authorisation. The Director of AGO is also required to provide the Minister with quarterly reports on the activities conducted in accordance with such approval. The accuracy of these and other reports provided to the Minister for Defence were reviewed during the reporting period by IGIS staff, and no issues were identified.

At the conclusion of approved activities, AGO staff prepare a post-activity compliance report for the Director, which this office examines. During 2018-19, IGIS staff identified no significant issues with these reports. However, the office noted one instance of non-compliance with the Ministerial Directions, whereby a Director's Approval was not approved at the appropriate level of delegation. This office subsequently recommended to AGO that it would be prudent to put in place a formal delegation procedure that makes clear the circumstances in which another officer may sign as acting Director. The office is satisfied that AGO has taken appropriate remedial action in response to this matter.

Protecting the privacy of Australians

The Minister for Defence issues written rules (the AGO Privacy Rules) to regulate how AGO communicates and retains intelligence information concerning Australian persons. During the 2018-19 reporting period IGIS staff did not identify any concerns in relation to AGO's compliance with the Privacy Rules. This is the third consecutive year in which AGO has been fully compliant with the AGO Privacy Rules.

7. Defence Intelligence Organisation

IGIS oversight of DIO in 2018-19 included inspections of DIO activities. IGIS received no complaints or public interest disclosures about DIO.

7.1 Inspections

During 2018-19, this office focused inspections on: assessments, advice and services; application of the Privacy Guidelines; record keeping; and training. The office's inspection of DIO's activities included following up on matters identified during the inquiry into the analytic independence and integrity of DIO conducted in 2017, as well as routine inspections of DIO's compliance with the *Guidelines to Protect the Privacy of Australian Persons*. IGIS staff also reviewed DIO's access to sensitive financial information from AUSTRAC. In addition to these inspection activities, the office attended relevant compliance training run by DIO, and monitored the percentage of DIO staff that have completed mandatory compliance training requirements.

Protecting the privacy of Australians

In 2018-19, IGIS staff reviewed DIO's compliance with its Privacy Guidelines twice. These guidelines, which are available on the DIO website, are similar to the Privacy Rules established under section 15 of the ISA for ASIS, ASD and AGO. They allow DIO to perform its role while protecting the privacy of Australians. This office did not identify any significant issues or concerns in this reporting period, and there was no evidence that DIO breached the Privacy Guidelines.

Attachment A: Role of the Inspector-General of Intelligence and Security

The Inspector-General is an independent statutory officer who reviews the activities of the following 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 Intelligence (ONI).

The Office of the IGIS is part of the Attorney-General's portfolio, and was previously located in the Prime Minister's portfolio from its commencement on 1 February 1987 until 10 May 2018. The IGIS is not subject to direction from any Minister on how responsibilities under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) should be carried out.

The *IGIS Act* provides the legal basis for the IGIS to conduct inspections of the intelligence agencies and to conduct inquiries of the Inspector-General's own motion, at the request of a Minister, or in response to complaints. The overarching purpose of the IGIS's activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights. A significant proportion of the resources of the Office are 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.

The inspection role of the IGIS is complemented by an inquiry function. In undertaking inquiries, the IGIS has strong investigative powers, including the power to require any person to answer questions and produce relevant documents, take sworn evidence, and enter agency premises. IGIS inquiries are conducted in private because they almost invariably involve classified or sensitive information, and the methods by which it is collected. Conducting an inquiry is resource intensive but provides a rigorous way of examining a complaint or systemic matter within an agency. The Inspector-General also receives and investigates complaints and public interest disclosures about the intelligence agencies. These come from members of the public and from current and former agency staff.

In response to the recommendations of the *2017 Independent Intelligence Review*, the Government announced that, subject to the introduction and passage of legislation, the jurisdiction of the IGIS will be extended to include the intelligence functions of the Department of Home Affairs, Australian Federal Police, Australian Criminal Intelligence Commission and Australian Transaction Reports and Analysis Centre. Resources for the IGIS have been increased to allow the office to sustain a full time equivalent staff of 55. As at 14 February 2020, the office had 33 staff (excluding the Inspector-General).