Review of Administration and Expenditure No. 20 (2020-2021)

Submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Christopher Jessup QC

Inspector-General of Intelligence and Security

25 March 2022

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 2020–21 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).

The Office of The Inspector-General of Intelligence and Security (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. To assist the Committee, this submission provides a summary of the key issues included in the IGIS 2020-21 Annual Report, and the Inspector-General would be pleased to assist the Committee with any further inquiries in a closed hearing.

Information about the role of the IGIS and the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act) is at **Attachment A**.

1.1 Approach to oversight activities and engagement

In general terms, for each agency within IGIS's jurisdiction, the relevant IGIS oversight team conducts inspections using a variety of methodologies. These include thematic reviews and risk-based random sampling. Each IGIS team also independently reviews agency self-reported compliance incidents. Inspection and other oversight activities are augmented by frequent contact with agency compliance staff and regular briefings on various matters, which assists IGIS staff to stay abreast of emerging issues, technologies, and to follow up observations from inspections.

In addition, 2020-21 formal triannual meetings with ASIO, ASIS, ASD and AGO were held between the Inspector-General, senior staff of IGIS and respective senior intelligence agency staff to discuss a selection of oversight-related matters. The Inspector-General also met with the Director-General, National Intelligence and the Chief Defence Intelligence.

2. Australian Security Intelligence Organisation

IGIS oversight of ASIO's activities in 2020-21 included inspections across a range of ASIO functions.

2.1 ASIO Inquiries

There were no Inquiries of ASIO in 2020-21. During the period, IGIS reviewed ASIO's implementation of the recommendation of the 2018 Inquiry into an ASIO matter. In June 2021, IGIS advised ASIO that it considered the eight inquiry recommendations to be fully implemented.

2.2 Inspections

The main inspection activities relating to ASIO included reviewing: ASIO's use of special powers under the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) and the *Telecommunications (Interceptions and Access) Act 1979* (the TIA Act) and other intelligence collection activities; its procedures relating to the quarantine and deletion of incidentally collected COVID app data; and ASIO's unlawfully intercepted information, security assessments, and advice to Ministers on security matters.

The following provides an unclassified overview of ASIO inspection and oversight activities by this office:

ASIO Act Warrants

IGIS review of ASIO Act warrants in 2020-21 included questioning warrants authorised by the Attorney-General after amendments to ASIO's compulsory questioning powers were enacted in December 2020. The compulsory questioning framework within the ASIO Act provides for IGIS oversight, including that the Inspector-General may be present at the questioning or apprehension of a person. Should the Inspector-General inform the prescribed authority of a concern about impropriety or illegality in connection with the exercise of powers under the warrant, the prescribed authority must ensure the concern is addressed satisfactorily. A person being questioned may make a complaint to IGIS (or the Commonwealth Ombudsman or relevant police complaints agency) and must be provided with the facilities to do so. IGIS must also be consulted on the preparation of a written statement of procedures to be following in the exercise of authority under a questioning warrant.

IGIS received several briefings from ASIO on its proposed use of the compulsory questioning powers and was consulted on development of the statement of procedures and ASIO's internal policy and procedures. For each questioning warrant issued by the Attorney-General, IGIS received the requisite notifications and information from ASIO. The Inspector-General attended the questioning sessions conducted during the reporting period and did not raise any concerns about impropriety or illegality during these questioning sessions.

Following questioning, ASIO notified IGIS of a potential breach of s 34DP of the ASIO Act concerning video recording of proceedings. This matter remained under investigation by ASIO at 30 June 2021.

During 2020-21, IGIS reviewed a small number of compliance incidents relating to the ASIO Act. One incident related to use of internally authorised tracking devices. New powers enacted in December 2020 enable ASIO to use certain types of tracking devices under internal authorisation rather than requiring a warrant to be authorised by the Attorney-General. ASIO reported an incident where it

considered that the request for an internally authorised tracking device may not have included the level of detail required to show that the legal threshold for authorisation had been met. ASIO's compliance review in response to the incident identified a number of weaknesses in ASIO's processes and made four recommendations directed at improving compliance with legislative requirements, providing a greater level of senior officer oversight, and strengthening collaboration between ASIO's legal and operational areas. IGIS conducted an independent review of the incident and agreed with ASIO's findings. As at 30 June 2021, IGIS had commenced reviewing ASIO's remediation action.

Interception warrants under the TIA Act

IGIS reviewed several breaches of s 7(1) and s 13 of the TIA Act that were proactively reported by ASIO. In addition, IGIS inspections identified one instance where a breach of s 7 had been identified and remedied but not reported to IGIS or the Attorney-General. IGIS was satisfied with ASIO's response to these incidents.

Access to telecommunications data under the TIA Act

IGIS inspected ASIO's access to telecommunications data. IGIS did not identify any issues of legality, but did find some procedural and record-keeping issues relating to internal approvals and the need for more detailed policy guidance relating to compliance reporting thresholds. IGIS will review the effectiveness of action taken by ASIO to address these issues in future inspections. In addition, IGIS reviewed nine compliance incidents reported in 2020-21 relating to authorisations under s 175 and s 176 of the TIA Act, as well as three incidents that had been reported the previous year. IGIS was satisfied with ASIO's proposed remediation action.

Special Intelligence Operations

During 2020-21, IGIS reviewed all special intelligence operations authorised by the Attorney-General. IGIS noted that ASIO had implemented feedback provided during earlier inspections and concluded that ASIO's management of its special intelligence operations was appropriate.

ASIO exchange of information with foreign authorities

In the last two years, IGIS has conducted dedicated inspections focussed on ASIO's exchange of information with foreign authorities. The first inspection identified improvements that could be made to better manage the potential human rights implications of disclosure. In the second inspection, IGIS reviewed changes to ASIO's policies and procedures made in response to the first inspection. IGIS was insufficiently assured that these changes were effective. ASIO has undertaken to further refine its policies and procedures and IGIS will examine this matter again during 2021-22.

Investigative cases

IGIS inspection of ASIO's investigative cases identified a number of matters that did not breach legislation but were noncompliant with the Minister's Guidelines or with internal policy and procedure. ASIO had proactively reported approximately 20 percent of these matters to IGIS. ASIO has since taken a number of steps to improve compliance, which IGIS will review during 2021-22.

Other inspections

In addition to the above inspections, IGIS conducted inspections relating to: analytic rigour and integrity; security assessments; ministerial submissions; Temporary Exclusion Orders; use of *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* powers; internal security investigations; exchange of information with Australian Government agencies; human sources; and the technical collection, retention, and deletion of data. These inspections did not identify significant concerns about legality or propriety, but in some instances identified matters for further attention by ASIO. The effectiveness of changes to ASIO's processes, policies and procedures will be reviewed during 2021-22.

The Minister's Guidelines

The Minister's Guidelines are issued under s 8A of the ASIO Act and are to be observed by ASIO in the performance of its functions. The Guidelines were issued in August 2020 and replaced the Attorney-General's Guidelines issued in 2007. IGIS assesses ASIO's compliance with the Guidelines across its inspection activities. IGIS also reviewed several breaches of the Guidelines relating to annual reviews of investigative cases and the collection, retention, use, handling, and disclosure of personal information.

3. Australian Secret Intelligence Service

IGIS oversight of ASIS's activities in 2020-21 included inspections across a range of ASIS functions.

3.1 ASIS Inquiries

There were no Inquiries of ASIS in 2020-21.

3.2 Inspections

The main inspection activities relating to ASIS included reviewing operational files and ministerial submissions. Operational file inspections primarily involved 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. Other inspection activities included access to sensitive financial information, and authorisations relating to the use of weapons and reporting of compliance matters.

The following provides an unclassified overview of these and other key ASIS inspection and oversight activities by this office:

Operational files

During the 2020-21 period this office reviewed files relating to ASIS's operational activities covering: four specific overseas locations; one sensitive intelligence activity; ASIS's management of large datasets (bulk data); activities conducted in relation to ASIO under s 13B of the *Intelligence Services Act 2001* (the IS Act); ASIS's management of human rights considerations; and ASIS's management of internal security investigations.

IGIS was satisfied that ASIS appropriately identified and considered legality and propriety risks associated with operational activities. In the context of these operational file inspections, IGIS highlighted several compliance concerns and other areas for improvement, particularly around timely and complete record keeping and procedural fairness processes related to internal security investigations.

Ministerial Submissions

IGIS reviewed the majority of ministerial submissions provided by ASIS to the Minister for Foreign Affairs as part of routine inspection activity. IGIS was satisfied that the information provided to the Minister was appropriate.

Ministerial Authorisations

IGIS reviewed all ministerial authorisations obtained by ASIS from the Minister for Foreign Affairs; this included three breaches of s 8 of the IS Act that ASIS self-reported where ASIS failed to obtain a ministerial authorisation before producing intelligence on Australian persons.

There were no emergency ministerial authorisations during the reporting period.

Section 15(5) and Privacy Rules

During 2020–21, ASIS reported five breaches of the Privacy Rules which constituted a breach of s 15(5) of the IS Act; these breaches occurred across three separate incidents. This is a significant reduction compared to the last reporting year, mainly because ASIS has developed a new automated process for publishing liaison reporting in a manner consistent with the Rules. IGIS was satisfied with ASIS's response to each incident.

Separately, ASIS self-reported a small number of other cases where, while there was no breach of the Privacy Rules, record keeping relating to the application of the rules was inadequate. IGIS looked at these cases and found no indication of systemic failings with ASIS's compliance controls or training.

Under the Privacy Rules, ASIS also advises IGIS when it obtains further information on an individual overseas that lead ASIS to overturn its initial presumption that the individual is not an Australian person. In 2020–21 ASIS reported five cases where such a 'presumption of nationality' was overturned. IGIS determined that in all cases ASIS's initial presumption was reasonable and in accordance with the Privacy Rules, as ASIS initially had no evidence that the individuals who were located outside Australia were Australian.

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 2020-21 period. IGIS also examined ASIS weapons and self-defence policies, guidelines and training records and did not identify any issues of concern. As at 30 June 2021, IGIS was conducting an inspection of weapons-related matters, which included reviewing ASIS's implementation of revised weapons guidelines.

4. Australian Signals Directorate

IGIS oversight of ASD's activities in 2020-21 included inspections across a range of ASD functions.

4.1 ASD Inquiries

During the period IGIS commenced an Inquiry into a complaint relating to ASD pursuant to subsection 8(2) of the IGIS Act. This Inquiry is ongoing.

4.2 Inspections

The main inspection activities relating to ASD included reviewing: applications for ministerial authorisation to produce intelligence on Australian persons; ASD compliance with the ASD Privacy Rules; compliance incident reports; and ASD's access to sensitive financial information.

The following provides an unclassified overview of these and other key ASD inspection and oversight activities by this office:

Ministerial Authorisations

The IS Act requires that ASD obtains authorisation from the Minister for Defence before conducting certain activities, including producing intelligence on Australian persons. During the period, IGIS inspected a sample of ASD's applications for ministerial authorisation which were found to be generally of a high standard.

The IS Act also requires that ASD provide the Minister for Defence with a written report in respect to each activity carried out in reliance on a ministerial authorisation. In 2020-21, IGIS reviewed the details of these reports to ensure ASD reports were accurate and furnished to the Minister in a timely manner. IGIS did not identify any significant issues with post-activity reports; however, IGIS did suggest ASD consider including additional detail about activities undertaken under ministerial authorisation to ensure that the Minister for Defence is more comprehensively informed about the activities conducted.

There were no emergency ministerial authorisations during the reporting period.

Ministerial Submissions

During 2020-21, IGIS conducted a quarterly review of a sample of submissions ASD provided to the Minister for Defence to ensure the Minister is provided accurate and timely information about critical ASD issues. During the period, and following on from an audit by ASD into ministerial submissions, ASD updated its governance arrangements for preparing submissions in support of ministerial authorisation, including regular audits to ensure the accuracy of information included in submissions. IGIS reviewed ministerial submissions and identified three instances where ASD was found to have provided the Minister for Defence with imprecise advice. These inaccuracies did not substantively influence the overall advice but highlighted the need for stringent assurance processes.

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 concerning Australian persons. During the period,

IGIS found that ASD's actions were in accordance with the ASD Privacy Rules, except for two incidents described below.

Firstly, ASD advised IGIS that information on an Australian person was retained due to a technical issue in contravention of ASD's intention to delete the information. An IGIS review of the matter post-incident revealed that ASD's remedial actions, including deletion of the information, were effective and appropriate in the circumstances. Under the ASD Privacy Rules, ASD also advises IGIS when it obtains further information on an individual that leads ASD to overturn its presumption that the individual was not an Australian person. If the initial presumption was reasonable, such incidences do not represent a breach of legislation or the Privacy Rules.

The second matter also involved a presumption of nationality issue and IGIS is currently reviewing the circumstances of the case to determine whether the requirements of the ASD Privacy Rules or IS Act were breached.

Legislative non-compliance

ASD often self-reports 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 IGIS.

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 authorising interception. In 2020-21, three instances of legislative non-compliance with the TIA Act occurred.

In two instances, ASD advised that, due to either technical or human error, it had intercepted or dealt with communications that were not authorised for interception under warrant. In the first instance, a technical error resulted in the unauthorised interception of communications. In the second instance, ASD did not cease interception despite being aware that unauthorised collection of communications might occur. While no unlawful interception was identified in the second case, ASD nevertheless failed to comply with para 7(1)(c) of the TIA Act by enabling unauthorised interception to occur. IGIS's review of both matters found the ASD's actions, including remedial actions taken following discovery of the incidents and updates to procedures, were appropriate in the circumstances.

As of 30 June 2021, ASD had confirmed a further non-compliance with the TIA Act, but had not yet finalised its investigation into the matter. ASD keeps IGIS briefed regarding these ongoing matters to ensure IGIS is informed on the progress of investigations.

In addition to the instances of non-compliance above, ASD also advises IGIS of matters where, during the course of lawful interception of foreign communications under warrant, ASD unknowingly and unintentionally enables interception of communications other than foreign communications. ASD has adopted safeguards to mitigate the occurrence of such incidents and informs the minister when they occur. Six such cases were reported to the IGIS during this reporting period.

IS Act Incident Reports

During 2020-21, ASD advised IGIS of two instances relating to compliance with the IS Act. In one instance, ASD advised that an activity conducted by the Australian Cyber Security Centre (ACSC) fell

outside the scope of ASD's functions. Part of ASD's cyber security functions requires the ACSC to work with industry to take down websites identified as malicious. In this case ACSC issued a takedown request before it had confirmed whether the website was malicious or not. In response to this incident IGIS made a number of recommendations and ASD undertook a range of measures including training and development of new standard operating procedure. IGIS's review of this incident found that the remedial actions taken by ASD were appropriate in the circumstances.

The second incident related to the requirement for the Minister to be satisfied that arrangements are put in place by ASD to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the performances of ASD's functions. In this case, the Minister was advised that such arrangements were in place; however, ASD subsequently advised that, due to human error, these arrangements were not in place at the time the activity was conducted. ASD has since undertaken remedial action to mitigate the risk of recurrence and IGIS is reviewing the matter to determine whether a breach of the IS Act has occurred.

5. Australian Geospatial-Intelligence Organisation

IGIS oversight of AGO's activities in 2020-21 included inspections across a range of AGO functions.

5.1 AGO Inquiries

There were no Inquiries of AGO in 2020-21.

5.2 Inspections

The main inspection activities relating to AGO included reviewing: applications for ministerial authorisation to produce intelligence on Australian persons; Director's Approvals and post-activity reporting; AGO compliance with the AGO Privacy Rules; and AGO's access to sensitive financial information.

The following provides an unclassified overview of these and other key AGO inspection and oversight activities by this office:

Ministerial Authorisations

The IS Act 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 2020-21, IGIS reviewed a majority of applications made by AGO for ministerial authorisation. IGIS inspections did not identify any issues related to the lawfulness or propriety of AGO activities during the period. Similarly, IGIS inspected a sample of AGO's written reports to the Minister for Defence on the activities it undertook under ministerial authorisation, to ensure reporting is accurate and provided in a timely manner. IGIS detected no significant issues with reports during the period. IGIS did suggest AGO consider including additional detail about activities undertaken under ministerial authorisation to ensure that the Minister for Defence is more comprehensively informed about the activities conducted.

There were no emergency ministerial authorisations during the reporting period.

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. During 2020-21, IGIS reviewed Director's Approvals and relevant documentation and no issues were identified. IGIS also examined post activity compliance reports submitted to the Director of AGO and no issues were identified with these reports.

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 2020-21 reporting period IGIS did not identify any instances of noncompliance in relation to AGO's compliance with the Privacy Rules.

6. Defence Intelligence Organisation

IGIS oversight of DIO's activities in 2020-21 included inspections across a range of DIO functions.

6.1 DIO Inquiries

There were no Inquiries of DIO in 2020-21.

6.2 Inspections

DIO inspections include compliance with measures to protect the privacy of Australians, and ensuring analytic integrity. IGIS also conducts other review and oversight related activity, including engaging with DIO on draft policies to identify compliance concerns and receiving briefings on new activities and initiatives.

Privacy rules inspections primarily involve reviewing DIO records relating to any collection or communication of identifiable information regarding Australian persons or entities. Inspections to examine analytic integrity focus on intelligence production and standards of analytic rigour and independence.

The following provides an unclassified overview of these and other key DIO inspection and oversight activities by this office:

Compliance with privacy guidelines

DIO has a set of Privacy Guidelines signed by the Minister for Defence that allow it to perform its role while respecting the privacy of Australians. They are similar to the Privacy Rules required for ASD and ASIS and are published on the DIO website.

During the 2020-21 period, IGIS undertook a complete audit of records relating to DIO's compliance with rules to protect the privacy of Australians. IGIS also cross-checked these records against its own independent monitoring of published product. The inspection found one case where there was a significant delay in the application of the guidelines and DIO subsequently reviewed the relevant policies to provide clearer direction.

Ensuring analytic integrity

In 2020-21, IGIS examined large numbers of published products and associated records to confirm independence of assessment and analytic rigour. The majority of the records were of a high standard and there were no issues of significant concern.

7. Office of National Intelligence

IGIS oversight of ONI's activities in 2020-21 included inspections across a range of ONI functions and were supplemented by briefings on emerging issues of interest, and proactive review of programs to evaluate risk.

7.1 ONI Inquiries

There were no Inquiries of ONI in 2020-21.

7.2 Inspections

ONI inspections included adherence to privacy rules designed to protect the privacy of Australians, analytic integrity, and the collection of open source information. Activities are examined for any legality or propriety concerns, and to ensure they demonstrate respect for human rights.

Privacy rules inspections primarily involve reviewing ONI records relating to any collection or communication of identifiable information regarding Australian persons or entities. Inspections to examine analytic integrity focus on intelligence production and standards of analytic rigour and independence. Open source inspections concentrate on those activities conducted under ONI's open source collection and analysis mandate.

The following provides an unclassified overview of these inspections:

Compliance with the Privacy Rules under s 53 of the ONI Act

During the 2020-21 period, IGIS reviewed files relating to ONI's compliance with rules to protect the privacy of Australians. IGIS also cross-checked these records against its own independent monitoring of published product. IGIS identified two products where the rules should have been applied but were not. IGIS considered these were isolated instances and not indicative of a systemic problem. IGIS also identified instances where administrative processes were not completed within policy timelines. The disjointed working arrangements necessitated by COVID-19 appeared to be the main hurdle in these instances. ONI has refined its policy guidance to guard against recurrence.

Ensuring analytic integrity

Section 12(2) of the *Office of National Intelligence Act 2018* (the ONI Act) affirms that ONI is not subject to direction regarding its intelligence judgements. During the 2020-21 period, IGIS examined large numbers of published products and associated records for evidence of demonstrated independence and analytic rigour. The majority of the records were of a high standard and no significant concerns were identified.

The collection of open source information

As well as traditional all-source assessment, ONI is responsible for the collection and analysis of open source material, and this has been an area of increasing intelligence focus. The 2020-21 inspection found a strong professionalised foundation for open source analysis and confirmed authorised staff undertook open source collection.

Leading the national intelligence community

During 2020-21, IGIS conducted its first inspection into the functions of ONI relating to leading the NIC. The review focused on foreign engagement, and intelligence coordination and evaluation. IGIS found no legality or propriety concerns with these activities.

8. Complaints and Disclosures

The IGIS 2020-2021 Annual Report notes that IGIS received 344 complaints and 16 public interest disclosures. Of the 344 complaints received, 167 were determined to be within IGIS jurisdiction.

In its last report, the Committee indicated its ongoing interest in the impact of changes to the practice of handling complaints about visa and citizenship matters that are lodged with IGIS.[1] As noted in the IGIS 2020-21 Annual Report, there was a significant reduction in the number of complaints received about visa and citizenship applications during the reporting period (from 300 in 2019-20 to 124 in 2020-21). The decrease in the number of visa and citizenship complaints received is likely due to COVID-19 travel related restrictions, particularly for international students. While it could be anticipated that complaints about these matters will increase in the current financial year (due to a relaxation in these boarder restrictions), IGIS is yet to observe such an increase.

IGIS would be happy to provide further information as required by the Committee in a closed hearing.

In its last report, the Committee indicated its ongoing interest in the impact of changes to the practice of handling complaints about visa and citizenship matters that are lodged with IGIS.[2] As noted in the IGIS 2020-21 Annual Report, there was a significant reduction in the number of complaints received about visa and citizenship applications during the reporting period (from 300 in 2019-20 to 124 in 2020-21). The decrease in the number of visa and citizenship complaints received is likely due to COVID-19 travel related restrictions, particularly for international students. While it could be anticipated that complaints about these matters will increase in the current financial year (due to a relaxation in these boarder restrictions), IGIS is yet to observe such an increase.

[1] Parliamentary Joint Committee on Intelligence and Security, *Administration and Expenditure Review No. 19 (2019-2020)*, paras 2.198-2.200.

[2] Parliamentary Joint Committee on Intelligence and Security, *Administration and Expenditure Review No. 19 (2019-2020)*, paras 2.198-2.200.

9. Other Inquiries

Two additional projects of interest to the Committee were undertaken by IGIS during the reporting period.

9.1 Preliminary Inquiry

In response to an August 2020 PJCIS recommendation, IGIS conducted a preliminary inquiry (s 14 of the IGIS Act refers) into each of the intelligence agencies' application of national security classifications. On 26 February 2021, the Inspector-General provided the PJCIS with a report of the preliminary inquiry, which concluded that no significant issues were identified and that a formal Inquiry was not necessary in relation to this matter.

Two recommendations were made for agencies within IGIS's jurisdiction: to ensure written guidance about security classifications is up to date and accessible, and to regularly review internal training so that staff are adequately supported to make classification decisions. The preliminary inquiry report is available on the IGIS website.

9.2 COVID app data

In 2020, IGIS established a project to identify those agencies within its jurisdiction that were most likely to collect COVID app data incidentally, and to determine if those agencies were complying with the protections and exemptions of Part VIIIA of the *Privacy Act 1988* (the Privacy Act). IGIS is undertaking this project in cooperation with the Australian Information Commissioner who, under the Privacy Act, has independent oversight responsibilities of the COVIDSafe app.

Part VIIIA sets out offences for the collection, use, and disclosure of COVID app data. Part VIIIA also provides an exception to the offence of collecting COVID app data where that collection occurs incidentally to the collection of lawfully intercepted information. No offence is committed if the incidentally collected COVID app data is deleted as soon as practicable after an agency becomes aware that it has been collected, and if the data has not been accessed, used or disclosed after it was collected. These protections and exemptions are of particular relevance for IGIS oversight of the activities of intelligence agencies.

During 2020-21, the Inspector-General provided the Australian Information Commissioner with two reports on the assurance activities undertaken by IGIS officers: 16 May 2020 to 16 November 2020, and 16 November 2020 to 15 May 2021.

The first report concluded that IGIS was satisfied that the relevant agencies had policies and procedures in place and were taking reasonable steps to avoid intentional collection of COVID app data. The report foreshadowed that IGIS inspections would verify data deletion and provide further assurance that no COVID app data has been accessed, used, or disclosed.

The second report similarly concluded that the relevant agencies were taking reasonable steps to avoid intentional collection of COVID app data and that appropriate procedures for incidental collection remained in place and continued to be followed. The report noted that relevant agencies have incidentally collected COVID app data, which the Privacy Act recognises may occur. No evidence was found to suggest that agencies have deliberately targeted or have decrypted, accessed, or used such data. Further, the Inspector-General found that relevant agencies were taking reasonable steps

to quarantine and delete such data as soon as practicable after the agency became aware of its collection. Finally, IGIS noted that discussions were ongoing between relevant parties about the application of the prohibition against 'disclosure' as set out in s 94D of the Privacy Act.

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).

In addition, the *Surveillance Legislation (Identify and Disrupt) Act 2021* expanded the Inspector-General's jurisdiction to include oversight of the use of network activity warrants by the Australian Criminal Intelligence Commission and the Australian Federal Police.

IGIS is an independent agency within the Attorney-General's portfolio. As at 30 June 2021, IGIS had 35 staff employed under the Public Service Act 1999. The Inspector-General is an independent statutory officer appointed under the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act) and therefore not an employee.

The overarching purpose of the IGIS's activities is to provide assurance 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 IGIS 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 IGIS Act provides the legal basis for IGIS to conduct inspections of the six intelligence agencies listed above and to conduct inquiries into the agencies of the Inspector-General's own motion, at the request of a Minister, or in response to complaints. The Prime Minister can request the Inspector-General to conduct an inquiry into an intelligence or security matter relating to any Commonwealth agency.

The inspection role of the IGIS is complemented by an inquiry function. In undertaking inquiries, the IGIS has 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. The Inspector-General also receives and investigates complaints and public interest disclosures about the six intelligence agencies within the Inspector-General's jurisdiction.