
# Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

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

The Hon Margaret Stone AO FAAL

Inspector-General of Intelligence and Security

25 October 2019

## Contents

## 1. Introduction

The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make this submission to the review by the Parliamentary Joint Committee on Intelligence and Security (the Committee) of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Assistance and Access Act). Information about the role of the IGIS is at **Attachment A**.

This submission does not make any comment on the policy underlying the Act, but identifies a number of issues that are relevant to effective and efficient oversight under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act). This submission supplements the submissions to the Committee on the then Bill in 2018 (the **2018 Bill Review**), and the Act earlier this year (the **2019 Act Review**). Previous IGIS submissions covered all parts of the Assistance and Access Bill and Act. This submission now focuses on the powers introduced by Schedule 5 and Schedule 2.

## 2. Summary of submission

As a matter of principle, IGIS is of the view that oversight is greatly assisted when laws providing agencies new and intrusive powers are clear, precise and unambiguous in their terms, and in their interaction with other powers. Clarity in decision-making criteria, limitations and the time period within which such powers may be exercised, are critical measures in overseeing intelligence agencies for legality and propriety. Oversight is further assisted by statutory record keeping requirements. Without legal certainty on these matters, oversight of, and public assurance about, agencies' use of these powers may be reduced.

Many of IGIS's earlier concerns about Schedule 1 (Industry assistance measures) of the Assistance and Access Act have been addressed by amendments made in December 2018. However, IGIS continues to hold concerns, particularly in relation to the two new powers granted to ASIO under Schedule 5: voluntary assistance requests (section 21A) and compulsory assistance orders (section 34AAA).

IGIS has monitored agencies' use of powers under the Assistance and Access Act, and continues to monitor resourcing constraints and the availability of independent technical expertise to provide advice on complex technical matters under the Act (such as the application of the systemic weakness limitation).

As part of its role, IGIS oversees ASIO's compliance with Guidelines issued by the relevant Minister. The ASIO Guidelines were last issued by the Attorney-General in 2007, before the widespread adoption of smartphone technology and end-to-end encryption, and before the introduction of a mandatory data retention regime. Since that time, ASIO has been granted a range of significant powers, and has exercised these powers in a changing security and technological environment. IGIS supports the ASIO Guidelines being reviewed and re-issued, in consultation with this office, as a matter of priority.

# 3. Issues arising from implementation

## 3.1 Resourcing

IGIS reiterates earlier evidence[1] that it will eventually be necessary for IGIS to have at least five additional staff (full-time equivalent) in order to conduct appropriately thorough and rigorous oversight of the new powers. While this need has been met temporarily from existing resources, this will be difficult to sustain if, in accordance with the recommendation of the 2017 Independent Intelligence Review, the IGIS Act is amended to expand the jurisdiction of the IGIS to the intelligence functions of a further four agencies in the national intelligence community.

Assessing whether the new powers granted under the Assistance and Access Act are used legally and with propriety will be assisted by access to independent technical expertise. For example, oversight of the industry assistance measures will require an assessment of the systemic weakness limitation that applies under the Act. While this expertise has not been engaged to date, IGIS is continuing to monitor the adequacy of resourcing and other arrangements, and will keep the Committee apprised of developments.

## 3.2 Implementation matters

As the Department of Home Affairs publicly acknowledged in its submission to the Committee's current review, Commonwealth law enforcement and national security agencies have used the powers under the Assistance and Access Act.[2] To the extent that these powers have been reviewed to date, the provisions enabling oversight by this office have been effective. If the Committee would find it helpful, IGIS could privately brief the Committee on matters that have arisen from oversight work undertaken by this office.

### 3.2.1 Administrative Guidance on industry assistance powers

In July, the Department of Home Affairs publicly released the *Administrative Guidance for agency engagement with designated communications providers* (Administrative Guidance) on the use of certain powers under the Act. The Administrative Guidance relates only to the powers contained in Schedule 1 of the Assistance and Access Act (new Part 15 of the *Telecommunications Act 1997*).[3]

IGIS was consulted in the development of this document, and continues to engage with the Department on a number of matters. IGIS continues to work collaboratively with the Department of Home Affairs as the policy department with responsibility for the Act, as well as agencies with powers under the Act, in the development of guidance and practices.

### 3.2.2 Attorney-General's Guidelines to ASIO

The *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating*

---

1 IGIS, *PJCIS 2019 Act Review—Submission 1.1,* p. 3; *PJCIS 2018 Bill Review*, *Committee Hansard*, Canberra, 27 November 2018, p. 5.

2 Department of Home Affairs, *PJCIS Act Review—Submission 16*, p. 14.

3 Department of Home Affairs, *Industry assistance under Part 15 of the Telecommunications Act 1997 – Administrative Guidance for agency engagement with designated communications providers*.

*intelligence relevant to security* (ASIO Guidelines) are issued under section 8A of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act).

The ASIO Guidelines were last issued in 2007, before the widespread adoption of smartphone technology and end-to-end encryption, and before the introduction of a mandatory data retention regime. Since that time, ASIO has been granted a range of intrusive powers, and has exercised these powers in a changing security and technological environment. IGIS has been involved in intermittent consultation over several years to update the Guidelines; however, new Guidelines have not been finalised. IGIS notes that the Committee made a recommendation in 2014 that the Guidelines be updated.[4]

The responsibilities of the IGIS extend to overseeing agency compliance with the Guidelines, and IGIS notes that the present Guidelines are long out of date, which detracts from their effectiveness. Updating the Guidelines gives an opportunity to address matters arising from changes in technology in the last decade, and other related issues including taking new technologies into account in assessing proportionality and intrusiveness. IGIS acknowledges that work is currently underway to modernise the ASIO Guidelines, and continues to work collaboratively with the relevant agencies on this matter. IGIS supports the ASIO Guidelines being reviewed and re-issued, in consultation with this office, as a matter of priority.

# 4. Submission

## 4.1 Schedule 5—ASIO voluntary assistance requests (ASIO Act, s 21A)

### Overview of the provisions

Schedule 5 of the Assistance and Access Act amended the ASIO Act to provide that the Director-General of Security (or his/her delegate) may issue a request for voluntary assistance (a ***voluntary assistance request***) to a person (whether a natural or a legal person) to assist ASIO with a broad range of activity. The scope of assistance that may be requested is broad and not limited to the technical assistance contemplated under Schedule 1 of the Assistance and Access Act (Part 15 of the *Telecommunications Act 1997*).

A voluntary assistance request is capable of covering:

- acts that are likely to yield only minor or peripheral assistance to ASIO in the performance of any of its functions (as well as acts that are likely to yield a substantial degree of assistance in the performance of functions, including assistance that is critical to identifying and responding to security threats that may not be possible without that assistance); and
- assistance that consists of the performance of one or more of ASIO's functions, such as the collection of intelligence, or the performance of services for ASIO that in some way helps ASIO

[4] Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the National Security Legislation Amendment Bill (No. 1) 2014*, September 2014, Recommendation 4. See also Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014,* February 2015, para 6.191 and 6.225.

> in the performance of its functions. This would seem to make it possible for an extension of civil immunity to 'ASIO affiliates'—a very broad range of persons.[5]

Whilst a voluntary assistance request under section 21A of the ASIO Act cannot be used to request a person to engage in criminal conduct, conduct undertaken in accordance with a request has immunity from civil liability provided that, among other things, the conduct does not 'result in significant loss of, or serious damage to, property'. The decision to grant immunity from civil liability is not a minor decision, as it will result in the loss of a right to a legal remedy for a person affected.

Amendments introduced and passed by the Parliament in December 2018 address some of the key concerns previously raised by IGIS.[6] However, IGIS has a number of outstanding concerns.

#### 4.1.1 Interaction with Technical Assistance Requests (Schedule 1 of the Assistance and Access Act)[7]

Assistance that may be rendered to ASIO under a voluntary assistance request (issued under section 21A of the ASIO Act) significantly overlaps with assistance that may be given pursuant to a Technical Assistance Request (TAR) (issued under Part 15 of the *Telecommunications Act 1997*—Schedule 1 of the amending Assistance and Access Act) in that both schemes carry immunity from civil liability for conduct done in accordance with the relevant request. However, a TAR also carries effective immunity from criminal liability for certain computer offences in Part 10.7 of the *Criminal Code*.

IGIS notes that the decision to issue a TAR is subject to the following issuing conditions, limitations and other safeguards, which are not applied to voluntary assistance requests:

- a TAR can only be issued to a 'designated service provider';
- a TAR cannot be issued to a person unless the request is reasonable and proportionate, and practicable and technically feasible;
- a TAR must satisfy manner and form requirements (including limitations on oral requests);
- a TAR must not result in systemic weakness or systemic vulnerability;
- a TAR cannot be issued for an activity that ASIO (or other authorised agency) would otherwise require a warrant; and
- the person must be informed that compliance with the TAR is voluntary.

A voluntary assistance request is not subject to equivalent limits, and the Committee may wish to examine further the justification underpinning this difference in approach.

---

5 'ASIO affiliate' means a person performing functions or services for the Organisation in accordance with a contract, agreement or other arrangement, and includes a person engaged under section 85 and a person performing services under an agreement under section 87, but does not include the Director-General or an ASIO employee. *Australian Security Intelligence Organisation Act 1979* (ASIO Act), s 4.

6 In the PJCIS review of the Bill, IGIS expressed concern regarding notification requirements and form requirements (IGIS, *PJCIS Bill Review—Submission 52*, pp. 57-59). In the PJCIS review of the Act, IGIS provided evidence that the amendments passed addressed some of these concerns (IGIS, *PJCIS Act Review—Submission 1.1*, p. 9).

7 These comments supplement the following earlier evidence to the Committee: IGIS, *PJCIS Bill Review—Submission 52*, pp. 55-56; IGIS, *PJCIS Act Review—Submission 1.1*, p. 10; IGIS, *PJCIS Act Review—Submission 1.2,* p. 13.

### 4.1.2 Grant of immunity from civil liability and other matters

#### No requirement to consider reasonableness and proportionality in the grant of immunity[8]

Conferring immunity from civil liability is a significant power, as it deprives a third party of a legal right to a remedy. IGIS notes that the legislation is largely silent on the factors that must be considered by the decision-maker when making a voluntary assistance request under section 21A. In particular, the legislation does not impose any requirement for the Director-General of Security (or his/her delegate) to give specific consideration to the reasonableness and proportionality of the immunity that applies to conduct in accordance with the request for voluntary assistance. This is in contrast to proportionality requirements in the statutory authorisation criteria applying to the Attorney-General for ASIO's Special Intelligence Operations, which also confer civil immunity on participants. The Committee may wish to consider whether this should be addressed in the legislation.

Further, the civil immunity which section 21A(1) provides is broader than that provided in respect of the Special Intelligence Operation regime,[9] with fewer issuing conditions and limitations. A voluntary assistance request made by the Director-General is not subject to equivalent statutory decision-making criteria, statutory limitations, or a statutory requirement to keep written records of reasons.

The Committee may wish to consider whether the legislation should provide that the reasons for making a request should be required to be documented. That is, when making a written request under section 21A(2A), or a record of an oral request under section 21A(3), the reasons for making of the request, and considerations of the effect of the conduct requested (including that of immunity) are captured in a written record. Such a record would materially assist this office in subsequent oversight of the exercise of the power.

#### Other Matters

IGIS notes that the legislation does not contain provisions to guide the maximum period of effect for a voluntary assistance request, nor provisions relating to the way that such requests may be varied or revoked. The Committee may wish to consider whether such provisions should be included in the legislation.

## 4.2 Schedule 5—Compulsory assistance orders (ASIO Act, s 34AAA)

#### Overview of the provisions

Schedule 5 of the Assistance and Access Act also amended the ASIO Act to provide that the Attorney-General may make an order requiring a person to provide information or assistance that is reasonably necessary to allow ASIO to access data held in, or accessible from, a computer or data storage device that is the subject of, or is found, removed or seized, under a separate ASIO warrant. This could include biometric information that would assist in the access to the relevant data. Although possibly unclear on the face of the legislation,[10] IGIS understands that ASIO will still require a warrant

---

8 These comments supplement the following earlier evidence to the Committee: IGIS, *PJCIS Bill Review—Submission 52*, pp. 53; IGIS, *PJCIS Act Review—Submission 1.1*, pp. 3, 10; IGIS, *PJCIS Act Review—Submission 1.2,* p. 11.

9 ASIO Act, pt III, div 4.

10 Subsection 34AAA(1) enables the Director-General of Security to request the Attorney-General to make an order for the purpose of accessing data held in, or accessible from, a computer or data storage device that is

(the underlying warrant) for access to the data or device to which the compulsory assistance order relates.

Compliance with a compulsory assistance order could be required at any point where a warrant is in force, which would include the period before it is executed, during its execution, and after it has been executed. However, section 34AAA could also be interpreted to require compliance where the underlying warrant ceases to be in force, as the assistance order is not required to be limited to the timeframe for the underlying warrant. Non-compliance with an order is an offence, and attracts a penalty of five years' imprisonment, or 300 penalty units, or both.

### 4.2.1 Notification and service of orders[11]

IGIS notes that there is no requirement for a compulsory assistance order to be served on the person who is the subject of the order. This leaves open the possibility that a person may be in breach of an order of which that person is ignorant. For clarity, it may be advisable to provide that such an order is not enlivened until it is served on the person.

More generally, IGIS is concerned to ensure that the relevant requirements are specified clearly on the face of the provision. This is to facilitate compliance by ASIO, promote consistency of practice, ensure fairness and transparency for persons who are subject to those orders, and provide a clear benchmark for IGIS to conduct oversight. The Committee may also wish to consider whether a copy of the record of any oral request should be required to be provided to the Attorney-General to ensure that it accords with the oral request.

### 4.2.2 Specification of essential matters[12]

IGIS notes that, unless a compulsory assistance order relates to a device that is accessed wholly remotely under a warrant, there is no requirement for a compulsory assistance order to inform the person of:

- the place at which they must attend; or
- the period of time during which they must render assistance; or
- the 'information' or 'assistance' the person is obligated to render; or

---

associated with a warrant under section 25, 25A, 26 or 27A of the ASIO Act, associated with an authorisation made under an identified person warrant, or seized during a search of a person detained under a questioning and detention warrant. Subsection 34AAA(2) enables the Attorney-General to make the order either under paragraph (a), in a case where the computer or data storage device is associated with a warrant under section 27A (i.e. a foreign intelligence warrant); or under paragraph (b), 'in a case where paragraph (a) does not apply'. IGIS understand that, in either case, there will need to be an underlying warrant in place. However, IGIS notes the Department of Home Affairs' submission to the current review, which appears to indicate that paragraph 34AAA(2)(b) enables the Attorney-General to make an order in the absence of a warrant, if satisfied of certain criteria. See Department of Home Affairs, *Submission 16*, para 156 to 159.

[11] These comments supplement the following earlier evidence to the Committee: IGIS, *PJCIS Bill Review—Submission 52*, p. 64; IGIS, *PJCIS Bill Review—Submission 52.1*, p. 9; IGIS, *PJCIS Act Review—Submission 1.1*, p. 11; IGIS, *PJCIS Act Review—Submission 1.2*, p. 20.

[12] These comments supplement the following earlier evidence to the Committee: IGIS, *PJCIS Bill Review—Submission 52*, pp. 61-62; IGIS, *PJCIS Bill Review—Submission 52.1*, p. 9; IGIS, *PJCIS Bill Review—Submission 52.2* (entirety); IGIS, *PJCIS Act Review—Submission 1.1*, p. 11; IGIS, *PJCIS Act Review—Submission 1.2,* pp. 16-17.

- any other conditions the Attorney-General has imposed on the order.

In the absence of this information, IGIS notes that it may not be possible to imply a compliance period into a compulsory assistance order based on the period for which the underlying warrant is valid. As noted previously, the legislation appears to contemplate that information and assistance could be compelled while an underlying warrant is in force but *before* it is executed, and *after* a warrant has been executed and ceases to be in force.

IGIS remains of the view that it would be preferable, for both compliance and oversight, if all compulsory assistance orders were expressly required to specify, to the extent possible, a compliance period; the form of assistance required; and, where assistance is required in person, the place at which that assistance is to be provided. In addition, this would provide a stronger and more consistent safeguard for persons who are subject to an assistance order, so that they can readily ascertain and understand obligations and potential criminal liability.

### 4.2.3 Right to liberty of person and freedom from arbitrary arrest and detention[13]

IGIS notes that, in the absence of judicial oversight, there may be insufficient statutory safeguards against the risk of compulsory assistance orders requiring a person to attend a place to provide assistance resulting in an arbitrary arrest or detention. IGIS notes that a person departing a place at which they are compelled to provide assistance will commit an offence under the provision, and section 34AAA does not impose a time limit on the duration of which a person is required to attend a place to provide assistance. IGIS acknowledges previous evidence provided to the Committee that section 34AAA is not intended to be used as a basis for deprivation of liberty,[14] but considers that the current wording of the provisions could be considered ambiguous.

The Committee may wish to consider this further to ensure that an assistance order could not be exercised in a manner that would result in an arbitrary deprivation of liberty. IGIS notes that the measures that apply to the questioning and detention warrants framework, such as the IGIS's express powers to enter a place where a person is being detained,[15] were introduced, in part, to ensure against arbitrary arrest or detention. To mitigate the risk of arbitrary arrest or detention, the Committee may wish to consider a requirement for all compulsory assistance orders to specify the place and duration of a person's attendance, and for a statutory maximum duration for a person's attendance to be introduced.

### 4.2.4 Cessation of action where issuing grounds no longer exist[16]

IGIS notes that there is no obligation on the Director-General of Security to immediately take all necessary steps to cease executing a compulsory assistance order if the underlying warrant has expired or if the issuing grounds have otherwise ceased to exist. Subsection 34AAA(3D) obliges the Director-General to inform the Attorney-General if satisfied that the grounds on which an order was

---

13 These comments supplement the following earlier evidence to the Committee: IGIS, *PJCIS Bill Review—Submission 52*, p. 64; IGIS, *PJCIS Act Review—Submission 1.1*, p. 11; IGIS, *PJCIS Act Review—Submission 1.2,* pp. 16-18.

14 Department of Home Affairs, *PJCIS Act Review—Submission 16.1*, pp. 17-18.

15 IGIS Act, ss 9B, 19A.

16 These comments supplement the following earlier evidence to the Committee: IGIS, *PJCIS Bill Review—Submission 52*, p. 63; IGIS, *PJCIS Act Review—Submission 1.1*, p. 11; IGIS, *PJCIS Act Review—Submission 1.2,* p. 20.

made have ceased to exist, and subsection 34AAA(3E) obliges the Attorney-General to revoke the order if satisfied that the grounds on which the order was made have ceased to exist. However, unlike the obligation that applies to ASIO's special powers warrants,[17] there is no immediate obligation on the Director-General to take such steps as are necessary to ensure that action under the order is discontinued. That is, the Director-General of Security may be obliged to cease executing the underlying special powers warrant, but is not required to cease any accompanying compulsory assistance order to effect that same warrant unless and until the order is revoked by the Attorney-General.

Similarly, there is no requirement for the Director-General of Security to delete records or copies of information obtained under an assistance order, if the Director-General is satisfied that it is no longer required for the purpose of ASIO's functions and powers. This is an obligation under section 31 of the ASIO Act in relation to information obtained under an underlying special powers warrant. However, not all information obtained under a compulsory assistance order will be covered by section 31 (for example, log-in credentials to a computer, or biometric information).

The Committee may wish to consider these matters further, including whether amendments should be introduced to provide that a compulsory assistance order ceases to have effect when the underlying warrant also ceases to have effect, as well as measures relating to the retention of data acquired under an assistance order that is no longer required.

#### 4.2.5 Warrant reports

IGIS notes that amendments introduced in December 2018 extended ASIO's reporting requirements, and that compulsory assistance orders will be reported to the Attorney-General in connection with the underlying warrant under section 34 of the ASIO Act. Warrant reports greatly assist IGIS in overseeing ASIO's use of its powers, and are used by this office in its inspection activities.

However, IGIS notes that there is no time limit within the ASIO Act for such a report to be furnished. This differs from warrant reports under section 17 of the *Telecommunications (Interception and Access) Act 1979*, for which the applicable timeframe is three months. There is also no requirement for the warrant report to provide information on how the compulsory assistance order was executed by ASIO.[18] IGIS is of the view that oversight would be assisted if a warrant report was required to be produced in a specified timeframe, and include the following matters:

- what 'information' and/or 'assistance' was required under the order;
- whether the order has been satisfied;
- when the order was served on the person; and
- whether the information or assistance satisfied the reason for which the order was issued (i.e. whether the assistance provided ASIO the access it required).

[17] ASIO Act, s 30(1)(b).

[18] ASIO Act, s 34(1A) only requires the report to include 'details of the extent to which compliance with the order has assisted the Organisation in carrying out its functions'.

## 4.3 Schedule 2—ASIO computer access warrants

### Overview of the provisions

Schedule 2 of the Assistance and Access Act amended ASIO's existing computer access warrants framework under the ASIO Act.[19] Key changes included new powers that permit ASIO to:

- undertake **telecommunications interception** for the purposes of doing any thing specified in the computer access warrant (which would otherwise require a separate warrant under the *Telecommunications (Interception and Access) Act 1979*); and
- temporarily **remove a computer** or other thing from the premises for the purpose of doing any thing specified in the underlying warrant; and
- do things that **conceal access** to a computer, including for up to 28 days after the underlying warrant ceases to be in force.

While amendments introduced and passed by the Parliament in December 2018 address some of the key concerns previously raised by IGIS,[20] IGIS has an outstanding concern with these provisions.

### 4.3.1 Limitation on warrant reporting[21]

Prior to the amendments made by the Assistance and Access Act, ASIO was required to report on the exercise of a removal power if the removal caused material interference with, or obstruction or interruption of, the lawful use of a computer or device. The amendments made by the Assistance and Access Act extended the reporting requirement to temporary removals which resulted in material inference, obstruction or interruption. However, it may be difficult to identify with any accuracy whether the temporary removal deprived a person an opportunity to use a device during the period of removal, and if so, the effect of the removal on the person.

IGIS continues to support the inclusion of a reporting requirement for all instances of temporary removals of computers or other things from warrant premises under computer access warrants. The absence of such a requirement will make oversight complex and inefficient:

- It will be very difficult to determine whether a temporary removal caused material interference with the lawful use of a computer. Arguably, given the centrality of computers in lawful, routine personal and business activities, any temporary deprivation may be likely to cause a material interference with lawful use.
- The absence of a specific reporting requirement for all removals may also mean that suitably detailed records may not be made (or may not be made consistently) of the reasons for, and duration of, each removal.

---

19 ASIO Act, s 25A—(Assistance and Access Act, Schedule 2, Items 1 and 18).

20 In the PJCIS review of the Bill, IGIS expressed concern regarding reporting on post-warrant concealment and extending equivalent safeguards for concealment activities as for computer access activities (IGIS, *PJCIS Bill Review—Submission 52*, pp. 39-51). In the PJCIS review of the Act, IGIS provided evidence that the amendments passed addressed some of these concerns (IGIS, *PJCIS Act Review—Submission 1.1*, p. 9).

21 These comments supplement the following earlier evidence to the Committee: IGIS, *PJCIS Bill Review—Submission 52*, pp. 45-46; IGIS, *PJCIS Act Review—Submission 1.1*, p. 4 and 10; IGIS, *PJCIS Act Review—Submission 1.2,* p. 10.

## 4.4 Schedule 1—Industry assistance

### 4.4.1 Ongoing matters of concern to IGIS

IGIS notes that oversight is always assisted where there is clarity in the criteria which apply to decision-making, the limitations that seek to govern the application of powers, and how new powers intersect with established powers and practices. These matters are central to the responsibility of this office to oversee the legality, propriety and human rights compliance of agency activities.

During its 2018 and 2019 reviews, IGIS provided substantial evidence to the Committee on matters of concern regarding Schedule 1. The outstanding concerns can be broadly grouped into three areas:

- issues relating to the consideration of the granting of immunity;
- improving clarity to ensure lawful and proper decision-making; and
- transparency matters to aid oversight.

IGIS does not seek to replicate this evidence here, but would be happy to provide any further information that the Committee may require.

## Attachment A

## Role of the Inspector-General of Intelligence and Security

The IGIS 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 discharged.

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 (section 8, IGIS Act). 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.