

UNCLASSIFIED



Telecommunications Legislation Amendment (International Production Orders) Bill 2020

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

The Hon Margaret Stone AO FAAL
Inspector-General of Intelligence and Security

4 May 2020

UNCLASSIFIED

UNCLASSIFIED

Table of Contents

1. Introduction.....	3
2. Summary of submission.....	4
3. IGIS role in oversight of international production orders	6
4. Observations.....	7
4.1 Threshold issues	7
4.2 Application process.....	12
4.3 Reporting and transparency	14
4.4 Destruction of data	16
4.5 Notifications, access and record keeping.....	17
4.6 Technical matters	19
Attachment A: Role of the Inspector-General of Intelligence and Security	21

UNCLASSIFIED

1. Introduction

The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make this submission to Parliamentary Joint Committee on Intelligence and Security's inquiry into the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (the Bill).

Consistent with established practices, the IGIS does not comment on the policy underlying the Bill. However, this submission discusses a number of matters that are relevant to IGIS's oversight of the provisions, and to which the Committee may wish to have regard.

This submission is limited to comment on the provisions relating to proposed international production orders for national security matters (the orders that may be sought by the Australian Security Intelligence Organisation (ASIO)). Other than by way of comparison, the submission does not comment on the similar powers proposed for the Australian Federal Police, Australian Criminal Intelligence Commission, state/territory law enforcement agencies and integrity commissions as these bodies are not within IGIS's jurisdiction.

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

UNCLASSIFIED

2. Summary of submission

In its review of the Bill, the Committee may wish to consider whether some amendment is desirable in relation to the following matters.

Threshold issues

- (i) The requirement in the international production orders (IPO) regime for two-step approval (consent by the Attorney-General and authorisation by an Administrative Appeals Tribunal (AAT) member) means **that a more rigorous process would apply to the issue of international orders than to domestic warrants** for similar types of information (see discussion at page 7).
- (ii) There is currently no statutory requirement for nominated members of the AAT to consider **privacy, proportionality and human rights** in deciding whether to issue any of the three categories of IPOs that may be sought in relation to national security (see discussion at page 8).
- (iii) The **threshold for ASIO to access a person's telecommunications data**, or the data of a group of people, is that doing so *'would be in connection with the performance by the Organisation of its functions'*. While this threshold is consistent with that for ASIO's domestic access to such data; in the more than 12 years since that threshold was introduced there has been a dramatic change in the level of privacy intrusion involved in access to telecommunications data (see discussion at page 9).
- (iv) The **ASIO Guidelines** which regulate ASIO's activities including use and retention of telecommunications information have not been revised in over 10 years. ASIO's statutory powers and the technology available to it have been increased significantly in that time (see discussion at page 10).
- (v) The current domestic data access regime provides specific **protections for journalists** that are not present in the proposed IPO scheme. (see discussion at page 11).

Application process

- (i) ASIO's domestic telecommunications warrant framework requires that the **Director-General personally apply** for telecommunications warrants, which ensures a high level of attention is given to each application. Recognising that the creation of an IPO regime may increase the overall number of applications, it may be necessary to expand the authority to Deputy Directors-General. However, it is a significant step to allow such authority to be conferred on **any ASIO officer regardless of seniority**, as the Bill proposes (see discussion at page 12).
- (ii) The Bill contains **no statutory guidance on what may constitute 'urgent circumstances'** for the purpose of permitting a telephone application (see discussion at page 13).
- (iii) It appears anomalous that there is **no requirement to provide the Attorney-General with the particulars of the 'urgent circumstances'** when seeking his or her consent by telephone, but the particulars do have to be provided to the AAT member at the time a telephone application is made (see discussion at page 13).

Reporting and transparency

- (i) It would assist oversight for ASIO to be required to **report comprehensively to the Attorney-General** on all international production orders (see discussion at page 14).
- (ii) Some form of public **statistical reporting on ASIO's use of the IPO regime** would make the operation of the scheme more transparent (see discussion at page 15).

UNCLASSIFIED

- (iii) The Committee may wish to seek **assurance that designated international agreements** entered into under the framework established by the Bill **will be made public** (see discussion at page 16).

Destruction of data

- (i) A **statutory requirement for a periodic review of the ongoing relevance of the data** collected under international production orders would make the Bill's requirement that 'where the Director-General of Security is satisfied that the information is not likely to be used for a relevant purpose, the record must be immediately destroyed' more effective. In IGIS' experience, similar provisions in existing legislation may be of little effect because such reviews may not be undertaken and thus the obligation to destroy data is not enlivened (see discussion at page 16).
- (ii) Further, the Committee may wish to consider **extending destruction obligations to telecommunications data** provided under an order (in addition to intercept and stored communications) (see discussion at page 17).

Notifications, access and record keeping

- (i) It would aid oversight if the Bill contained a requirement for ASIO to **notify the IGIS of all IPOs that are issued within three months**, with the option of other notification periods to be agreed to by the Inspector-General and the Director-General of Security (see discussion at page 17).
- (ii) To avoid any doubt about access it may be appropriate to provide **express authority for the IGIS to access the register of IPOs kept by the Australian Designated Authority**, to the extent that the register relates to IPOs issued in relation to national security (see discussion at page 18).
- (iii) The Bill's **requirement that ASIO retain certain records** could be amended to require that records must be kept for three years, *or* for as long as any of the data obtained under an IPO is retained, whichever is the longer. Noting that not all documents that must be prepared under the Bill are required under clauses 135 and 136 to be kept, it may be preferable that the Bill contain a general record retention obligation that requires ASIO to keep all relevant records for IGIS inspection (see discussion at page 18).

Technical matters

- (i) Clause 153 should be amended to **enable IPO information to be used, recorded or disclosed** for the purpose of 'an IGIS official exercising a power, or performing a function or duty, as an IGIS official', not only functions under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act). The IGIS has powers and functions under a number of Acts. (see discussion at page 20).
- (ii) To ensure efficient and effective administration of different oversight aspects of the scheme there should be an amendment to the IGIS Act to provide **explicit authority for IGIS officials to share information** with the Attorney-General's Department for the purpose of its role as Australian Designated Authority (see discussion at page 20).
- (iii) IGIS notes that the use of different **definitions** for the same terms in the *Telecommunications (Interception and Access) Act 1979* (TIA Act) may cause complexity and result in confusion in the proposed new international framework (see discussion at page 20).

UNCLASSIFIED

3. IGIS role in oversight of international production orders

The existing jurisdiction of the IGIS under IGIS Act will enable the IGIS to oversee the use which ASIO makes of the IPO regime. Oversight will not only extend to the requirements and limitations contained in the Bill, but also any obligations or limitations imposed by an international agreement so far as they apply to ASIO.

Appropriately, the IGIS will not have authority to oversee the Attorney-General's decision to consent to an IPO application, or the decision of a nominated member of the Security Division of the AAT to issue an IPO. Similarly, the IGIS will not oversee the activities of the Attorney-General's Department (in its capacity as the Australian Designated Authority); however, the IGIS intends to maintain visibility of IPOs obtained by ASIO as they progress through the Department's assessment process.

UNCLASSIFIED

4. Observations

4.1 Threshold issues

(i) 'Double-lock' authorisation of international production orders

Differing authorisation standards between IPOs and existing ASIO warrants

The differences between the authorisation framework for the proposed IPO regime and ASIO's existing warrant framework, and between IPOs in relation to telecommunications data and IPOs in relation to interception and stored communications, invite the Committee's consideration.

The Bill proposes that IPOs in relation to national security will be issued to ASIO by nominated members of the Security Division of the AAT. In the case of IPOs relating to interception or stored communications, the Attorney-General's prior consent is also required. In effect, this introduces a form of 'double-lock' mechanism for these types of IPOs, similar to arrangements under the United Kingdom's *Investigatory Powers Act 2016*.¹

These arrangements differ from the existing arrangements in the TIA Act, where ASIO warrants for interception of, or access to, telecommunications are issued by the Attorney-General.² Warrants under the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) are also (with few exceptions) issued to ASIO by the Attorney-General.³

IGIS understands that the proposed role of the nominated AAT member in issuing IPOs to ASIO is to ensure compliance with the requirements of the United States *Clarifying Lawful Overseas Use of Data Act* (the CLOUD Act).⁴ However, the effect is that IPOs will require a higher level of authorisation than for warrants to access the same data held in Australia. Although ultimately a matter of policy, it may be useful for the Committee to be aware of these differences between the existing domestic framework and the proposed international framework.

Unlike IPOs in relation to interception and stored communications, the Bill does not propose that ASIO needs the Attorney-General's consent to apply for an IPO in relation to telecommunications data. Rather, approval by a nominated member of the Security Division of the AAT will be required. The Explanatory Memorandum does not give reasons for this difference. The potential intrusiveness of telecommunications data is discussed in further detail below (page 9).

¹ The *Investigatory Powers Act 2016* (UK) provides that warrants for the interception of telecommunications cannot come into force until they have been approved by a Judge, following approval by a Secretary of State.

² The arrangements also differ from the Bill's proposed mechanism in relation to law enforcement agencies, for which an IPO may be issued by an eligible Judge or by a nominated AAT member.

³ The exceptions are questioning warrants, and questioning and detention warrants, which are issued by a judicial issuing authority with the Attorney-General's consent (ASIO Act, Part III, Division 3).

⁴ See ASIO (Submission 26), p. 3. The CLOUD Act requires that orders issued by a foreign government subject to an agreement with the United States must be 'subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order'.

UNCLASSIFIED

(ii) Consideration of privacy, proportionality and human rights

Statutory requirement to consider privacy and proportionality

The Committee may wish to consider a statutory requirement for nominated members of the Security Division of the AAT to consider privacy, proportionality and human rights in deciding whether to issue any of the three categories of IPOs that may be sought in relation to national security.

The Bill provides that, in deciding whether to issue an IPO at the request of a law enforcement agency, an eligible Judge or nominated AAT member must have regard to specific matters. These include:

- how much the privacy of any person or persons would be likely to be interfered with;
- the gravity of the conduct being investigated;
- how much the information that would be likely to be obtained would be likely to assist in connection with the investigation;
- to what extent other methods have been used by, or are available to, the agency;
- how much the use of those other methods would be likely to assist, or to prejudice, the investigation; and
- such other matters (if any) as the Judge or AAT member considers relevant.⁵

In contrast, a nominated member of the Security Division of the AAT deciding whether to issue an IPO at the request of ASIO is *only* required to have regard to a subset of these factors.⁶ In particular, the nominated member is not required to have regard to the privacy of any person or the gravity of the conduct being investigated, or the level of assistance that would be likely be provided to ASIO in carrying out its functions. The Explanatory Memorandum does not give reasons for this distinction.

IPOs issued to ASIO could potentially be very broad in scope, extending beyond individuals reasonably suspected of being engaged in acts prejudicial to security, to services used for ‘purposes prejudicial to security’.⁷

IGIS would expect ASIO to consider privacy and proportionality matters in its applications. The Attorney-General’s Guidelines, issued to ASIO under section 8A of the ASIO Act (discussed further below at page 10), require that any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence; and require ASIO to undertake its investigations using as little intrusion into individual privacy as is possible, consistent with the performance of its functions.⁸ However, the Attorney-General’s Guidelines do not extend to decisions made by members of the Security Division of the AAT. A statutory requirement for the nominated

⁵ Proposed Schedule 1, clauses 30(5)-(6), 39(3), and 48(5) regarding the issue of IPOs relating to enforcement of the criminal law. See also clauses 60(5)-(6), 69(3), and 78(5) for similar requirements regarding the issue of IPOs relating to control orders.

⁶ Proposed Schedule 1, clauses 89(5)(a)-(b); 98(3), 107(5).

⁷ Proposed Schedule 2, clauses 89(2)(e)(iii), (f)(iii).

⁸ *Attorney-General’s Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)* (the Attorney-General’s Guidelines), paragraph 10.4.

UNCLASSIFIED

member to consider privacy and proportionality in deciding whether to issue an IPO in relation to national security may give the public stronger assurance that these matters will be given due consideration by the decision-maker who issues the order. For similar reasons, and because the Bill contains little consideration of human rights, it may also be appropriate for there to be a statutory requirement for the nominated AAT member to consider human rights in deciding whether to issue an IPO.

(iii) Criteria for accessing telecommunications data

Threshold for applying for an IPO in relation to telecommunications data.

Given that the informative value and relative privacy intrusion of the data has increased significantly with technological advances, the Committee may wish to consider the threshold for applying for an IPO for telecommunications data.

An IPO for telecommunications data does not require the relevant person to be engaged in, or likely to engage in, activities prejudicial to security.⁹ Rather, the nominated member of the AAT Security Division must be satisfied that disclosing the telecommunications data to ASIO would be ‘in connection with the performance by the Organisation of its functions’.

While this is consistent with Chapter 4 of the TIA Act (the equivalent domestic authorisation scheme), IGIS notes that this domestic authorisation scheme is currently the subject of the Committee’s *Review of the mandatory data retention regime*. In a submission to that review, IGIS noted that the threshold for ASIO to access telecommunications data is ‘low’. This threshold was introduced more than twelve years ago (in 2007, the same year the iPhone was introduced) when the volume and nature of communications data held by carriers and carriage service providers was quite different.¹⁰ IGIS notes that the informative value and relative privacy intrusion of telecommunications data (including a person’s location history, and the details of the persons they contact) to both intelligence agencies and the public, has increased significantly with technological advances. IGIS notes that other countries with similar regimes have set a higher threshold for data access than the Bill. For example, the United States’ CLOUD Act limits any disclosure of communications or data to matters involving serious criminal offences and terrorism matters (which are indictable offences in Australian law).

As noted previously, the issuing authorities for an IPO requested by a law enforcement agency must have regard to a range of matters when deciding whether to issue an order, including expectations of privacy and the gravity of conduct. Importantly, this extends to all applications by law enforcement applications for IPOs, including for telecommunications data. IGIS again notes that these matters are not required to be considered by a nominated member of the AAT for an IPO requested by ASIO.

⁹ Proposed Schedule 1, clause 107.

¹⁰ Inspector-General of Security, *Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the mandatory data retention regime* (Submission 36), pp. 6, 9.

UNCLASSIFIED

(iv) Attorney-General's Guidelines to ASIO

Update on Attorney-General's Guidelines

The Committee may wish to seek an update on the revision of the ASIO Guidelines. IGIS supports the ASIO Guidelines being comprehensively updated, in consultation with this office, as a matter of priority.

The ASIO Act requires ASIO to observe Guidelines issued by the Minister in the performance of its functions and the exercise of its powers.¹¹ IGIS has previously advised the Committee of the need for the 2007 Attorney-General's Guidelines to ASIO to be updated to take into account the range of new intrusive powers, and the changed security and technological environment, since they were last issued more than a decade ago.¹² These Guidelines are publicly available and, if kept up to date, could provide the public with useful information about how ASIO operates and the standards that it must uphold when exercising its powers.¹³ The Committee also recommended in 2014 that the Guidelines be updated.¹⁴

This Office has been party to discussions with relevant departments and agencies concerning the revision of the ASIO Guidelines. More guidance could be provided on how proportionality is to be assessed and how the potential impact on third parties is to be taken into account by ASIO. Guidance relating to ASIO's access to and retention of personal information would also benefit from being updated. In addition, IGIS continues to be of the view that questions regarding the relative intrusiveness of access to different types of information should be addressed in the Guidelines.

If the current Bill passes into law, further changes to the Guidelines will be required to take into account the new types and volume of data that could be obtained under the proposed international framework, as well as the new reporting and application process.

¹¹ ASIO Act, section 8A(1).

¹² See Inspector-General of Intelligence and Security, *Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the mandatory data retention regime* (Submission 36), p. 12; *Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Submission 28), p. 5.

¹³ The Guidelines are publicly available at <<https://www.asio.gov.au/legislation.html>>. Comparatively, the UK has adopted six public codes of practice in accordance with the *Investigatory Powers Act 2016* that apply to the activities by UK intelligence agencies. These codes of practice, which have been approved by both Houses of Parliament, set out processes and safeguards for the use of investigatory powers by public authorities including bulk acquisition of communications data, intelligence services' retention and use of bulk personal datasets, equipment interference, interception of communications and national security notices. The six codes of practice can be accessed at <<https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice>>.

¹⁴ Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the National Security Legislation Amendment Bill (No. 1) 2014*, September 2014, Recommendation 4.

UNCLASSIFIED

(v) Protections for certain groups (e.g. journalists)

Extending additional protections that apply to existing communications access

The Committee may wish to consider whether the protections afforded to certain groups under Australia's domestic authorisation scheme, as well as the protections for other privileges, should apply to the proposed international production order scheme. If so, the Committee may wish to consider amendments that require an issuing authority to consider additional matters in relation to certain groups.

The Bill proposes to establish a new authority for agencies to be able to obtain the content of communications and telecommunications data of certain persons, in parallel with existing domestic regimes. However, some of safeguards that are afforded under Australia's existing domestic scheme for the same type of information do not appear in the Bill. For example, the domestic regime provides additional protections where ASIO or law enforcement agencies are seeking to access the telecommunications data of a journalist for the purpose of identifying another person whom is reasonably believed to be that journalist's source.¹⁵ These additional requirements were introduced into the domestic framework in recognition of the public interest in maintaining a journalist's confidentiality. By way of comparison, the United Kingdom's Overseas Production Orders legislation precludes orders including material which is subject to legal professional privilege and other confidential personal records,¹⁶ and has provided express protections for journalistic data.¹⁷

It may be intended that such protections be provided in relevant international agreements,¹⁸ and that they would apply to any IPO issued under the auspices of an agreement.¹⁹ As there is no legal requirement in the Bill or in Australian domestic law for this to be so, the Committee may wish to consider whether similar protections should be expressly extended to such groups as additional decision-making criteria for the relevant issuing authority. These could include existing protections (for example, the protections for journalistic data noted above, as well as those relating to parliamentary privilege and legal professional privilege). Such protections would only apply to Australian authorities requesting information from a communications provider located overseas, and would not bind incoming orders served on Australian communications providers. If the Committee wished for these protections to apply to incoming orders, additional amendments to the Bill would be required or additional provisions in a relevant international agreement.

¹⁵ *Telecommunications (Interception and Access) Act 1979* (TIA Act), Chapter 4, Division 4C.

¹⁶ *Crime (Overseas Production Orders) Act 2019* (UK), ss 1(3), (7) and 3.

¹⁷ *Crime (Overseas Production Orders) Act 2019* (UK), s 12.

¹⁸ As is appropriate, IGIS has not been party to the negotiations between the Australia and the United States as our two governments progress a bilateral agreement.

¹⁹ For example, the US' CLOUD Act provides that an order may not be used to infringe freedom of speech – a right that has a special extension to journalists in the US unlike in Australia (US CLOUD Act, § 2523, (b)(1)(E)). This would be a matter that the Australian Designated Authority would be required to be satisfied of in its consideration of an order's compliance with the international agreement.

UNCLASSIFIED

4.2 Application process

(i) Officers who may apply for international production orders

Limitations on who may apply for an international production order

The Committee may wish to consider whether the Bill should be amended to reflect ASIO's domestic telecommunications warrant framework so as to limit authority to apply for an international production order to the Director-General of Security.

If a limited delegation power was considered necessary, the Committee may wish to consider limiting delegations to a Deputy Director-General or Deputy Directors-General.

The Bill proposes to provide the Director-General of Security, a Deputy Director-General of Security or an ASIO employee (in relation to whom a specific authorisation is in force) with the right to make an application for an international production order.²⁰ There is no requirement in the Bill for the ASIO employee, or class of ASIO employees, be of a particular level of seniority or to possess particular qualifications. Nor does the Bill limit the scope of, or otherwise describe, the ASIO employees that could be authorised to apply for an IPO.

More generally, these provisions are a substantial departure from ASIO's existing domestic telecommunications warrant regime. In particular, ASIO's existing warrant framework provides that only the Director-General may apply for a warrant to intercept telecommunications or to access stored communications.²¹ This restriction reflects the significant intrusion into a person's privacy (and that of third parties with whom they communicate) that results from interception and access. Similarly, the Director-General's power to apply for warrants under the ASIO Act cannot be delegated.

IGIS acknowledges that the introduction of the IPO scheme may mean that the overall number of applications made by ASIO may increase, and that consequently it may not be practicable for the Director-General to continue to consider all applications personally. In which case, the proposed extension to permit a Deputy Director-General to make an application would ensure that there remains a very senior level consideration of the application for an IPO, should that be necessary.²² However, the reasons for granting similar powers to a class of ASIO employees of unspecified seniority or experience are not apparent on the face of the Bill, nor does the Explanatory Memorandum address this issue. IGIS notes that requesting the Attorney-General's consent to an IPO application, preparing an affidavit and ensuring compliance with an international agreement are substantial matters (potentially with significant legal consequences) that would ordinarily require very senior level consideration in ASIO.

If the Committee is minded to consider this matter the main issue is: whether there should be parity with the existing domestic ASIO warrant regime, limiting the power to apply for an IPO to the Director-

²⁰ For IPOs for interception: Proposed Schedule 1, clause 83; for IPOs for stored communications: Proposed Schedule 1, clause 92; for IPOs for telecommunications data: Proposed Schedule 1, clause 101.

²¹ TIA Act, s 9B.

²² Proposed Schedule 1, clauses 83(3)(b), 92(3)(b) and 101(3)(b).

UNCLASSIFIED

General; or whether the power should extend to Deputy Directors-General or other senior officers as well as the Director-General.

(ii) Urgent applications

‘Urgent Circumstances’

The Committee may wish to consider including statutory guidance on what will constitute ‘urgent circumstances’ for the purpose of a telephone application.

In any event, an amendment to provide that the particulars of the urgent circumstances which necessitate making a telephone application be communicated to the Attorney-General when seeking the Attorney-General’s oral consent would assist the Attorney in considering the application.

What constitutes an urgent circumstance?

The Bill does not set out what may constitute an urgent circumstance, and the Explanatory Memorandum does not provide guidance on this matter. The Committee may wish to consider whether the types of circumstances that would amount to ‘urgent circumstances’ should be set out in legislation—perhaps adopting the approach taken in the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, where a specific harm threshold was inserted for urgent requests or notices. That Act provides that technical assistance requests²³ and technical assistance notices²⁴ must not be issued orally unless:

- a) an imminent risk of serious harm to a person or substantial damage to property exists; and
- b) the request or notice is necessary for the purpose of dealing with that risk; and
- c) it is not practicable in the circumstances to give the request or notice in writing.

A similar statutory definition of ‘urgent circumstances’ could have several benefits: it would clearly articulate the Parliament’s expectations about when ‘urgent circumstances’ are considered to arise, provide legislative guidance to nominated members of the Security Division of the AAT when considering IPO applications, and promote consistent decision-making within ASIO when applying for IPOs.

Information given in a telephone application for ‘urgent circumstances’

IGIS notes that there appears to be a difference between the information required to be provided by ASIO to the Attorney-General and to the nominated AAT Security Division member in respect of an application for an IPO (for interception or stored communications) in urgent circumstances.

The Bill proposes that ASIO officers may make applications to a nominated member of the AAT’s Security Division by telephone where there are urgent circumstances.²⁵ A telephone application must

²³ *Telecommunications Act 1997*, ss 317H(2).

²⁴ *Telecommunications Act 1997*, ss 317M(2).

²⁵ Proposed Schedule 1, clauses 84, 93 and 102.

UNCLASSIFIED

include the particulars of the urgent circumstances that justify the making of the application orally.²⁶ In the case of telephone applications, the nominated member must be satisfied that, because of the urgent circumstances, it was necessary to make the application by telephone.²⁷

ASIO, however, is not required to provide this same information to the Attorney-General at the time of seeking the Attorney's oral consent.²⁸ Instead, such information is required to be provided in writing within three working days after the day on which the application was granted, withdrawn or refused by the nominated AAT member.²⁹

An amendment to provide that the Attorney-General is also advised orally of the particulars of the urgent circumstances which necessitate a telephone application would ensure that the Attorney-General is apprised of the 'full picture' in the same manner and timeframe as the nominated AAT member. The report, proposed in subclauses 83(10) and 92(9), could then formalise the oral advice provided to the Attorney-General, as well as advise the Attorney whether the application was granted, withdrawn or refused.

4.3 Reporting and transparency

(i) Reports to the Attorney-General

Extending Attorney-General reporting requirements

The Committee may wish to consider (a) extending the requirement to report to the Attorney-General to all IPOs; and (b) whether the matters on which ASIO is required to report to the Attorney-General should be expanded.

Written reports about action taken under a warrant are crucial to accountability and to effective oversight. They provide transparency to the Attorney-General which can inform the Attorney's decisions in relation to future applications. As an oversight body, the Office of the IGIS relies on these reports in reviewing ASIO's actions for legality and propriety.

The Bill provides that the Director-General must give a written report to the Attorney-General in respect of each IPO issued for intercepted communications within three months of its expiry, revocation or cancellation.³⁰ However, IGIS notes that the Bill currently provides that a report to the Attorney-General is *not* required for IPOs for access to stored communications or IPOs for telecommunications data. The Explanatory Memorandum does not give any reasons for this difference. To close this lacuna and to ensure consistency and accountability, IGIS suggests that written reports, within three months of expiry, should be provided to the Attorney-General for *all* IPOs, or at least those IPOs where the Attorney-General's consent is required prior to issue.

Further, while clause 129(a) requires ASIO to provide a report to outline how the information collected under an IPO for interception has assisted the Organisation in carrying out its functions, IGIS suggests

²⁶ Proposed Schedule 1, clauses 87, 96 and 105.

²⁷ Proposed Schedule 1, clauses 89, 98 and 107.

²⁸ Proposed Schedule 1, subclauses 83(9) and 92(8).

²⁹ Proposed Schedule 1, subclauses 83(10) and 92(9).

³⁰ Proposed Schedule 1, clause 129.

UNCLASSIFIED

that these reports should be required by statute to include more comprehensive reporting requirements, such as an explanation of what information or data was obtained (including any information or data relating to persons other than the subject of the IPO), how ASIO has used the information or data (including whether such information or data was shared with other agencies) and whether the data is still being retained (and, if so, why).

In relation to the sharing of information or data collected under an IPO, IGIS notes that clause 153 contains a range of exceptions for disclosure. These exceptions are tightly defined for law enforcement, but are broadly defined for ASIO (clause 153(h) provides that disclosure may occur in the performance of the functions, or exercise of the powers, of the Organisation). Such a broad secondary disclosure provision may emphasise the importance of more comprehensive written reports to the Attorney-General.

(ii) Annual reporting

Publication of statistics in annual report

The Committee may wish to consider whether it would be appropriate to require statistical reporting on ASIO's use of the IPO regime to be made public.

The Bill amends the ASIO Act to require that ASIO include a range of statistics on its use of the IPO regime in its annual report.³¹ Although unclassified portions of ASIO's annual report are required to be tabled in the Parliament, the Minister, on the Director-General of Security's advice, may make such deletions as he or she considers necessary in order to avoid prejudice to security, the defence of the Commonwealth, the conduct of the Commonwealth's international affairs, or the privacy of individuals.³² Statistics on ASIO's use of warrants and other powers are generally excluded from the public version of the report.

This approach contrasts with provisions for law enforcement agencies, for which the Bill includes a specific provision requiring statistics on each agency's use of the IPO regime to be included in a public annual report that is tabled in the Parliament and a scheme for reconsideration of a decision that it is necessary to exclude some information.³³ If it was considered necessary to allow the exclusion of certain information from ASIO's public reporting, the proposed scheme for reconsideration of such decisions for law enforcement could be extended to ASIO's reporting requirements.

The absence of public statistical reporting for ASIO contrasts with international approaches; for example, in the United Kingdom, where a wide range of statistics on the use of investigatory powers, including by intelligence agencies, is reported in the annual report of the Investigatory Powers Commissioner's Office.³⁴

³¹ Item 4 of the Bill.

³² ASIO Act, section 94(5).

³³ Proposed Schedule 1, clause 131. There are only narrow grounds upon which information can be excluded from this report – see clauses 131(3) and 132.

³⁴ Investigatory Powers Commissioner's Office, *Annual Report 2018*, Part 18, pp. 114-119, available at <<https://ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf>>

UNCLASSIFIED

(iii) Tabling international agreements

Tabling designated international agreements

The Committee may wish to seek assurance that designated international agreements entered into under the framework established by the Bill will be made public.

IGIS assumes that subclause 3(7) of proposed Schedule 1 will mean that any designated international agreement that is entered into for the purposes of the IPO framework will be tabled in the Parliament and made public. However, the Committee may wish to seek assurances that this will be the case, as this provision could be interpreted differently. IGIS would be concerned to be in a position where agencies are held accountable to standards that have not been made public. This would be likely to affect IGIS's statutory responsibility to assure the Parliament and the public that intelligence and security matters are open to scrutiny.

4.4 Destruction of data

Statutory requirement for periodic review of the relevance of data collected under international production orders

A statutory requirement that ASIO periodically review the relevance of data collected under IPOs would give effect to the Bill's requirement that, where the Director-General of Security is satisfied that the information is not likely to be used for a relevant purpose, the record must be immediately destroyed. The Committee may also wish to consider whether the Director-General's obligations in this regard should be delegable and whether the destruction obligations should be extended to telecommunications data provided under an international production order (in addition to intercepted and stored communications).

The Bill proposes that if the Director-General of Security is satisfied that information provided in compliance with an IPO for interception or stored communications is 'not likely to be used' for a relevant purpose (such as the performance of ASIO's functions and exercise of powers), the Director-General must cause the record to be immediately destroyed.³⁵ There is no such obligation in relation to IPOs for telecommunications data. IGIS has previously commented on this matter in a submission to the Committee's current *Review of the mandatory data retention regime*.³⁶

IGIS notes that these provisions are similar to the existing provisions in the TIA Act and the ASIO Act. There is no trigger for the Director-General to determine that a communication is 'not likely to be used', and in the absence of a requirement for the periodic review of the data provided under an IPO, the data may be retained indefinitely because a determination about its use has not been made.

As stated to the Committee in previous inquiries,³⁷ IGIS has observed during its inspections of ASIO records over several years that the lack of such a trigger means that a determination may not be made, and often data that has been ingested into ASIO's systems continues to be retained. Accordingly, the

³⁵ Proposed Schedule 1, subclauses 140(2) and (4).

³⁶ Inspector-General of Intelligence and Security, *Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the mandatory data retention regime* (Submission 36), pp. 13-14.

³⁷ Inspector-General of Intelligence and Security, *Submission to the Parliamentary Joint Committee on Intelligence and Security Review of the mandatory data retention regime* (Submission 36), pp. 13-14.

UNCLASSIFIED

Committee may wish to consider an amendment requiring the Director-General to consider periodically whether specific data is ‘not likely to be used’ and if not, to destroy the data. The Committee may also wish to consider whether the Director-General’s obligations in this respect should be expressly delegable in legislation (for example, to a Deputy Director-General or an authorised class of ASIO employee).³⁸

Finally, IGIS notes that clause 140 does not apply to IPOs for telecommunications data. The Committee may wish to consider an amendment to extend the destruction obligations to these orders.

4.5 Notifications, access and record keeping

(i) Notifications

General notification obligation with timing able to be varied administratively

The Committee may wish to consider a statutory obligation in the Bill for ASIO to notify the IGIS of all IPOs that are issued within three months, with the option to vary the notification periods by agreement between the Inspector-General and the Director-General of Security.

In previous submissions to the Committee, IGIS has noted the importance of notifications to this Office (periodic or individual) for efficient and effective oversight.³⁹ The Committee has also indicated the importance it places on notification provisions. For example, most recently, in its review of the then Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, the Committee recommended mandatory notification provisions. Amendments to this effect were introduced and passed. As a result, that Act requires ASIO to notify IGIS within seven days of issuing an industry assistance request or notice, regardless of the urgency of the assistance sought.⁴⁰

There are no equivalent notification requirements in the IPO Bill for ASIO to notify the IGIS, and the Committee may wish to consider an amendment to the Bill to provide for a statutory notification obligation. Noting that the frequency of ASIO’s use of IPOs may be difficult to quantify for some time, it may be sufficient for there to be a statutory obligation to notify IGIS within three months, with the option of other notification periods being agreed to by the Inspector-General and the Director-General. This could allow for bulk or batch-style reporting on a periodic basis, if necessitated by the quantity of orders issued.

³⁸ IGIS considers that a power to destroy data, unlike a power to seek an order to obtain it, does not have the same privacy implications for individuals and thus does not raise the same concerns about delegation.

³⁹ For example: Inspector-General of Intelligence and Security, *Submission to the PJCS Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Submission 52), p. 14.

⁴⁰ *Telecommunications Act 1997*, sections 317HAB, 317MAB and 317TAB.

UNCLASSIFIED

(ii) Access to the Australian Designated Authority's register

Statutory authority to access register held by Australian Designated Authority

The Committee may wish to consider amendments to provide express authority for the IGIS to access the register of IPOs kept by the Australian Designated Authority, to the extent that the register relates to IPOs issued in relation to national security.

The Bill requires the Attorney-General's Department, as the Australian Designated Authority, to keep a register of all IPOs issued under the regime.⁴¹ Although the IGIS does not have oversight of the Australian Designated Authority, access to this register (so far as it relates to IPOs issued in relation to national security) would assist the IGIS's oversight of ASIO's functions under the regime.

As discussed further below, an exception to the Bill's secrecy offence will allow the Attorney-General's Department to share relevant information with the IGIS. This intention has been confirmed by the Attorney-General's Department in its submission to the Committee.⁴² However, to avoid any doubt and to provide stronger ongoing assurance that the IGIS will have access, it may be preferable for the Bill to provide express authority for the IGIS to access the register of IPOs.

(iii) Record retention

Robust record retention requirements

The Committee may wish to consider the duration of the obligation to retain records, and whether all information and documents prepared for the operation of the regime should be statutorily required to be kept for IGIS inspection.

Under the Bill, ASIO must retain certain records for three years commencing when the document came into existence (clauses 135 and 136).

The record retention requirements for ASIO's domestic telecommunications warrants are regulated by a 2016 determination of the National Archives under the *Archives Act 1983*.⁴³ The determination specifies that records *related to* warrants for security intelligence collection may be destroyed from ten to 150 years after last action or must be retained indefinitely (depending on the class of record). IGIS notes that ASIO's recordkeeping in respect of its current warrant framework is of a high standard, and anticipates that similar standards would be maintained in respect of the IPO regime.

Nonetheless, IGIS considers that oversight is greatly assisted by clear legislative requirements for the retention of information. The Bill's requirement that ASIO retain certain records for three years could be enhanced by adding an additional requirement to provide that certain records must be kept for three years, *or* for as long as any of the data obtained under an IPO is retained, whichever is the longer.

⁴¹ Proposed Schedule 1, clause 139.

⁴² See Attorney-General's Department (Submission 16), p. 17.

⁴³ National Archives, Records Authority 2012/00324244, available at <https://www.naa.gov.au/sites/default/files/2019-12/agency-ra-2012-00324244.pdf>.

UNCLASSIFIED

This would ensure that there is a clear accountability record for data received under an IPO that is subsequently retained.

However, IGIS also notes that not all documents that must be prepared under the Bill are required by clauses 135 and 136 to be kept. For example, the documentation provided to the Attorney-General seeking consent to an application for an IPO, and a record of whether the Attorney-General consented to that application or refused consent, is *not* required to be retained.

IGIS considers that legislating a specific list of records that are required to be kept carries a risk that not all records associated with the administration of the IPO regime would be captured. The Committee may therefore consider it preferable that the Bill contain a general record retention obligation that requires ASIO to keep all relevant records for IGIS inspection. IGIS notes that the inspection regime undertaken by IGIS for ‘legality and propriety’ looks to a much wider range of information than the specific regime prescribed for inspections by the Ombudsman.

4.6 Technical matters

(i) Information sharing and secrecy offences

Amendments to secrecy provisions

The Committee may wish to consider:

- an amendment to clause 153 to enable IPO information to be used, recorded or disclosed for the purpose of ‘an IGIS official exercising a power, or performing a function or duty, as an IGIS official’.
- an amendment to the IGIS Act to provide explicit authority for IGIS officials to share information with the Attorney-General’s Department for the purpose of its role as Australian Designated Authority.

The Bill’s secrecy provisions make it an offence for a person to use, record, or disclose information about, or obtained in accordance with, an IPO,⁴⁴ with exceptions for a range of permitted purposes.⁴⁵

As noted earlier, it is envisaged that the IGIS will have visibility of ASIO’s IPOs as they progress through the assessment phase undertaken by the Attorney-General’s Department (as the Australian Designated Authority). This will be facilitated through an exception to the secrecy offence enabling IPO information to be used, recorded or disclosed for ‘the performance of a function or duty, or the exercise of a power, by an IGIS official under the [IGIS Act]’.⁴⁶ As noted by the Attorney-General’s Department in its submission, the exception will permit both ASIO and Attorney-General’s Department employees to share relevant information with IGIS,⁴⁷ including for the purpose of IGIS’s inspections, inquiries or in response to complaints about ASIO’s activities under the IPO framework.

⁴⁴ Proposed Schedule 1, clause 152.

⁴⁵ Proposed Schedule 1, clause 153.

⁴⁶ Proposed Schedule 1, clause 153(1)(p).

⁴⁷ See Attorney-General’s Department (Submission 16), p. 17.

UNCLASSIFIED

However, IGIS notes two limitations in the scope of this exception as drafted:

1. The exception at clause 153(1)(p) only extends to an IGIS official's functions, duties and powers under the IGIS Act. IGIS officials also have functions and duties under other pieces of legislation, including the ASIO Act, the *Freedom of Information Act 1982* and the *Public Interest Disclosure Act 2013*. Unnecessarily limiting the exception to functions and duties under the IGIS Act could limit our ability to respond appropriately to matters arising under each of those Acts in connection with ASIO's activities under the IPO regime. This limitation would be resolved if the exception was amended to enable disclosure for the purpose of 'an IGIS official exercising a power, or performing a function or duty, as an IGIS official'.
2. The exception at clause 153(1)(p) only extends to information being used, recorded or disclosed (for example, by the Attorney-General's Department) in support of IGIS's functions. Given that IGIS and the Attorney-General's Department will have oversight roles for different parts of the process for ASIO IPOs, IGIS may need to work closely with the Department to ensure that the respective roles are effective. This may, at times, require IGIS to share information with the Department in support of its functions. Under the secrecy offence at section 34 of the IGIS Act, however, it is an offence for an IGIS official to divulge to any person information acquired under the IGIS Act by reason of the person being an IGIS official, except in the performance of his or her functions or duties or in the exercise of his or her powers under the IGIS Act (or other named Acts). A broadly drafted amendment to the IGIS Act, providing explicit authority for IGIS officials to share information with the Attorney-General's Department for the purpose of its role as Australian Designated Authority, would achieve the necessary level of certainty for IGIS and the Attorney-General's Department to cooperate in this manner.

(ii) Consistency of definitions

Consistency of definitions

Different definitions for the same terms may cause complexity and result in confusion in the proposed new international framework.

IGIS notes that several of the definitions used in the Bill differ from existing definitions in other parts of the TIA Act. Examples include the definitions of 'carrier' and 'carriage service provider'. The Bill also introduces a definition of 'telecommunications data', which is a term used but not defined in other parts of the TIA Act. The Committee may wish to consider any practical ramifications that may arise as a result of these differences. More generally, having different definitions for the same terms within the same Act creates complexity in legislation and may cause confusion. The confusion may extend beyond agencies' use of the domestic and international regimes, but also to Australian communications providers who are required to apply different legal tests in providing data to Australian authorities under the domestic regime, as well as any incoming IPOs from a foreign government with whom Australia has a relevant cross-border data access agreement. A statutory review of the provisions after a set period of operation may provide an opportunity to address any issues that arise as a result of these differences.

UNCLASSIFIED

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.