IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Dr James Renwick CSC, SC
Independent National Security Legislation Monitor
3-5 National Circuit
BARTON ACT 2600

Dear Dr Renwick

Thank you for the opportunity to provide a submission to your review of the Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018.

As you may be aware, my office has made several submissions over the past twelve months to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for its reviews of the Telecommunications and other Legislation Amendment (Assistance & Access) Bill 2018 (TOLA Bill), and of the subsequent TOLA Act.

To assist your review, I enclose copies of the following submissions to the PJCIS:

- Review of the TOLA Act (statutory review required by section 187N of the TIA Act)
  - *Submission 28*, dated 25 October 2019
- Review of the TOLA Act (2018 referral by the Senate)
  - *Submission 1*, dated 6 December 2018
  - *Submission 1.1*, dated 21 January 2019
  - *Submission 1.2*, dated 13 February 2019
- Review of the TOLA Bill (2018 referral by the Attorney-General)
  - *Submission 52*, dated 12 October 2018
  - *Submission 52.1*, dated 23 November 2018
  - *Submission 52.2*, dated 29 November 2018

I would welcome the opportunity to discuss the contents of these submissions in person, should you require.

If I can be of any further assistance, please contact my office. The contact officer for this matter is [redacted], who can be reached on [redacted].

Yours sincerely

[redacted]

Margaret Stone AO FAAL
Inspector-General

29 October 2019

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.

UNCLASSIFIED

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Correspondence ref: OIGIS/OUT/2018/1296 File ref: 2018/141

Mr Andrew Hastie MP, Chair
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Dear Chair,

Thank you for giving me the opportunity to comment on the recommendations made by the Parliamentary Joint Committee on Intelligence and Security in relation to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (the Bill). I also thank the Committee for giving such careful consideration to the oversight implications of new powers contained in Schedule 1 to the Bill. I recognise that the recommendations of the Committee are made in the context of the Committee accepting that there is a:

> … genuine and immediate need for agencies to have tools to respond to the challenges of encrypted communications [and that the] absence of these tools results in an escalation of risk and has been hampering agency investigations over several years.

It is in response to this need that the Committee has recommended that the Parliament pass the Bill, with amendments, as soon as possible, with further reviews to be initiated immediately by the Committee and subsequently by the Independent National Security Legislation Monitor (INSLM). Given this urgency and the further scheduled reviews, I make these comments:

- I have reviewed the proposed Government amendments as circulated this morning (amendment sheet EK171, 9:22 am) and am satisfied that, in the context of urgency and planned review, the Government amendments satisfactorily address my concerns on the issues noted in recommendation 5.
- I particularly welcome the addition of notification requirements in relation to new powers in Schedules 1 and 5, and some amendments to reporting requirements in Schedules 2 and 5. These notifications will allow us to target our oversight or the new powers more effectively and make it more efficient and effective. Nevertheless overseeing these new powers will still be complex and resource intensive.
- I welcome recommendation 17 and consider that the first limb of that recommendation (amendments in relation to s 317ZG) has been implemented in full. However, in relation to the second limb of recommendation 17, there may need to be some further amendments to ss 317ZH(1) and (4) to account for ASIS and ASD's use of technical assistance requests.

1 National Circuit BARTON ACT 2600 Phone (02) 6271 5692 E-mail info@igis.gov.au

- There are a number of other matters raised in my submissions to the Committee that have not been addressed in the amendments however, given the urgency and opportunities for further reviews of the legislation in line with recommendations 14 and 16, these additional matters could be dealt with satisfactorily in Ministerial Guidelines, at least as an interim measure. I have suggested that the Ministerial Guidelines made under s 8A of the ASIO Act be updated accordingly and have said I would be happy to work with ASIO and the Department of Home Affairs in the development of revised Guidelines.
- I anticipate that ASIO (and to lesser extent ASIS and ASD) will need to develop detailed internal policies and procedures applicable to the exercise of new powers particularly those conferring broad discretions; I am happy to be consulted by agencies in the development of these policies and procedures.

Assuming the Bill is passed, I plan to divert resources within my office from oversight of other agencies to oversight of ASIO's use of the new powers in Schedules 1, 2 and 5. I hope to be able to make the results of that oversight available to the Committee and the INSLM to assist in their proposed reviews.

Yours sincerely

[redacted]

Margaret Stone
Inspector-General

6 December 2018

UNCLASSIFIED

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Supplementary submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone

Inspector-General of Intelligence and Security

21 January 2019

Introduction

The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make this supplementary submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Act) with specific reference to Government amendments introduced and passed on 6 December 2018. Information about the role of the IGIS is at **Attachment A**.

This submission responds to an invitation to provide certain additional information following the commencement of the Act on 9 December 2018. It supplements the Inspector-General's correspondence to the Committee of 6 December 2018 (received as submission 1 to this inquiry).

IGIS response to PJCIS recommendation 5 on the Bill

The Inspector-General's correspondence of 6 December 2018 responded to recommendation 5 of the Committee's report on the Bill. The Committee recommended that IGIS and Ombudsman should provide assurances directly to the Committee that the amendments to the Bill agreed to by the Government address their concerns about the matters listed in that recommendation:

- *explicit notification and reporting requirements when issuing, varying, extending or revoking a notice or request under Schedule 1;*
- *limits on the exercise of Schedule 1 powers (including extending prohibition on systemic weakness to voluntary notices, ensuring decision-makers consider necessity and intrusion on innocent third parties when issuing a notice);*
- *defences for IGIS officials; and*
- *clear information sharing provisions.*

IGIS commented, in summary, that:

- Given the urgency, the Government amendments implementing the Committee's recommendations on Schedule 1 (and the matters of defences for IGIS officials and information-sharing as relevant to provisions in Schedules 2 and 5) satisfactorily addressed the concerns raised by IGIS about the particular matters identified in recommendation 5. IGIS also welcomed the further Government amendments to Schedules 2 and 5 (ASIO powers) that addressed some, but not all, of the additional concerns identified in our evidence to the Committee.
- A number of IGIS's other concerns about Schedules 1, 2 and 5 (which were not the subject of specific recommendations in the Committee's report on the Bill) were not implemented in the Government amendments. IGIS noted that, as an interim measure, these matters could be dealt with in the *Minister's Guidelines to ASIO* made under section 8A of the *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*) pending further reviews. IGIS would oversee ASIO's compliance with the amended guidelines in exercising the new powers.
- Oversight of ASIO's use of the new powers (and to a lesser extent, the use by ASIS and ASD of technical assistance requests) would nonetheless be complex and resource intensive for IGIS.

Implementation of the amendments

Oversight, including resourcing

Information about IGIS involvement to date in overseeing the new powers is provided in a classified annexure. IGIS is also aware that agencies are currently updating, or are intending to update, their internal documentation to support the exercise of the new powers. IGIS anticipates being consulted on these in due course.

While it is too early to comment meaningfully on the whether the provisions are conducive to effective oversight (by reference to practical experience) IGIS has directed resources to developing oversight methodologies for the new powers, and will keep the Committee apprised.

IGIS remains of the view provided in the Inspector-General's evidence to the Committee in 2018 that it will eventually be necessary for IGIS to have approximately five additional staff (full-time equivalent) in order to conduct appropriately thorough and rigorous oversight of the new powers.[1] While this need can be met temporarily from existing resources, this will be difficult to sustain when the *IGIS Act* is amended to confer jurisdiction on IGIS for the oversight of the intelligence functions of a further four agencies in the national intelligence community. It will also be necessary to monitor the adequacy of resourcing and other arrangements continuously, so that IGIS has appropriate access to independent technical expertise.

Amendments to the Minister's Guidelines to ASIO

IGIS has not received any indication from ASIO or the Department of Home Affairs as to whether amendments to the *Minister's Guidelines to ASIO* are being prepared to implement, at least on an interim basis, the large number of matters identified in IGIS's submissions on the Bill that were not included in the Government amendments to the Bill. Without amendments to the Guidelines, these matters remain unaddressed, either directly in primary legislation or in administratively binding guidelines made under the *ASIO Act*. (The key outstanding concerns are summarised below.)

Outstanding IGIS concerns not addressed in the Act

IGIS has a number of outstanding concerns about Schedule 1 (industry assistance scheme), Schedule 2 (ASIO computer access warrants) and Schedule 5 (ASIO power to grant civil immunities to persons providing voluntary assistance, and a new scheme of compulsory assistance orders).

These concerns are detailed in **Attachment B** (Schedule 1) and **Attachment C** (Schedules 2 and 5). Of these, the most significant concerns are about Schedule 5 and to a lesser extent Schedule 2.

Key outstanding concerns in relation to Schedule 5 (assistance to ASIO)

Immunities from civil liability for persons assisting ASIO: ASIO Act, s 21A(1)

- **No proportionality assessment:** The Director-General of Security (or delegate) is not required by the Act to be satisfied that the conferral of civil immunity is reasonable and proportionate, as a precondition to granting the immunity. (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.)

1 IGIS, *Committee Hansard*, 27 November 2018, p. 5.

- **No exclusion of certain harmful conduct:** The immunity is not subject to an exclusion for conduct causing significant financial loss, or serious physical or mental harm to a person. (The exclusions in s 21A(1) apply only to significant loss of or damage to property, and conduct involving the commission of an offence.)
- **No maximum period of effect:** Requests for voluntary assistance, and consequently the civil immunity, are not subject to any maximum period of effect.

Compulsory assistance orders: ASIO Act, s 34AAA

- **Not all assistance orders are required to specify essential matters:** an assistance order is only required to specify certain essential matters (the compliance period, place of attendance and conditions on the order) if a computer has been removed from premises under a warrant. If a computer is accessed wholly remotely under a warrant, there is no requirement for orders to specify these matters, which may reduce transparency.
- **Arbitrary deprivation of liberty**: there are no express safeguards against the risk that an order requiring a person to attend a place to provide assistance may result in an arbitrary deprivation of liberty.
- **No obligation to cease action taken under an order where issuing grounds no longer exist:** the Director-General of Security is not subject to a statutory requirement to take all reasonable steps to cease executing an assistance order, if he or she is satisfied that the issuing grounds have ceased to exist. (This is in contrast to a statutory obligation in relation to warrants.)

Key outstanding concern in relation to Schedule 2 (ASIO warrants)

- **Limitation on warrant reporting—temporary removals of computers and other things:** Warrant reports under s 34 of the *ASIO Act* are not required to identify specifically whether a computer or other thing was removed from premises. Existing reporting requirements in s 34 will only apply if ASIO makes an assessment that a temporary removal of a computer or thing caused material interference with the lawful use of a computer. This will make it difficult for IGIS to oversee the exercise by ASIO of the new temporary removal powers, including ASIO's decision making about whether a removal caused a material interference.

IGIS views

IGIS continues to support the express inclusion of all outstanding matters in primary legislation or, at least as an interim measure, in Ministerial guidelines made under the *ASIO Act*. It is particularly important for the key issues listed above to be addressed promptly, as they are critical to the effective oversight of the new and expanded powers in Schedules 2 and 5 to the Act.

In conducting its present review of the Act, or potentially in its later statutory review, the Committee may wish to consider whether some or all of these matters should be pursued; and if so, the appropriate vehicle for giving effect to them (both immediately and in the longer term).

IGIS notes that placing these matters solely in Ministerial guidelines has the potential to be more expeditious than legislative means, if those guidelines are made promptly. It may also maximise flexibility in making future amendments to accommodate changes to operational circumstances. However, including at least the key parameters in primary legislation (with further, more procedural details able to be set administratively) may provide a stronger degree of clarity, certainty and parliamentary oversight. (This would include Parliamentary approval of future amendments through the passage of amending legislation, including any proposals to repeal the original provisions.)

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) (formerly the Office of National Assessments).[2]

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 Office has 27 staff at 21 January 2019.

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.[3] 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. IGIS staff have access to all documents of the intelligence agencies, and the IGIS is often proactively briefed about sensitive operations.

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 are being increased to allow the office to sustain a full time equivalent staff of 55 (by 2019-20) and to allow the agency to move to new premises (in 2019).

---

2 *Office of National Intelligence Act 2018* and *Office of National Intelligence (Consequential and Transitional Provisions) Act 2018* (commenced 20 December 2018).

3 See *IGIS Act,* section 8 in relation to the general jurisdiction of the IGIS.

Attachment B

Implementation of IGIS concerns included in recommendations 5 and 17

PJCIS recommendation 5

The Committee recommends that the Bill be amended to incorporate suggestions from the Office of the Inspector-General of Intelligence and Security (IGIS) to strengthen oversight of the powers in Schedule 1 of the Bill, as it applies to the Australian Security Intelligence Service (ASIO), the Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD).

This includes:

- ***explicit notification and reporting requirements when issuing, varying, extending or revoking a notice or request under Schedule 1;***

Partially implemented

Addressed in Government amendments

- ✓ Notification of issuing, extending or revoking TAR, TAN or TCN.
- ✓ Notification of IGIS when a TCN consultation request issued.
- ✓ Requirement to inform a DCP of their right to complaint to IGIS in relation to a TAN (but not the execution of a TCN).
- ✓ Provision of assessor's report to IGIS.
- ✓ Classified statutory annual reporting by ASIO (numbers issued).

Not implemented

- × No annual reporting by ASIS and ASD.
  (This could be done administratively. IGIS has not been advised of any commitment to do so.)
- × No notification of IGIS by ASIO, ASIS or ASD if a provider does an act under a TAR, TAN or TCN in reliance or purported reliance on the civil or criminal immunity that causes significant loss, damage, injury or interference with lawful computer use (and annual reporting of statistical information about these instances, on a classified basis if necessary).

- ***limits on the exercise of Schedule 1 powers (including extending prohibition on systemic weakness to voluntary notices, ensuring decision-makers consider necessity and intrusion on innocent third parties when issuing a notice);***

Partially implemented

Addressed in Government amendments

- ✓ Prohibition on TARs requesting the creation or non-remediation of systemic weaknesses or vulnerabilities.
- ✓ Proportionality requirement in issuing, variation and revocation criteria for TARs, TANs, TCNs, including a requirement to consider impacts on some third parties *(however, this is only those persons who are not of interest to intelligence agencies).*
- ✓ Fixed maximum period of effect for TANs and TCNs *(however, this does not apply to TARs, which are only subject to a 90-day maximum if the TAR does not specify an expiry date.).*

Continued

Not implemented

- ✗ No express requirement for persons issuing TARs, TANs and TCNs (as applicable) to consider the potential impacts of an immunity on **all** third parties who may be affected by the DCP's actions under the request or notice; only the those persons who are **not** of interest to ASIO (in relation to TARs, TANs and TCNs) or ASIS or ASD (in relation to TARs).
- ✗ No fixed maximum period of effect for TARs. *(90-day maximum in s 317HA(1) applies only if the TAR does not specify an expiry date. There is no limit on the expiry date that can be specified.)*
- ✗ No statutory clarification of overlap between TARs and ASIO s 21A(1) requests.
- ✗ No further limitations on civil immunities (exclusion of conduct causing serious financial loss, damage to property, personal injury or harm, or an offence).
- ✗ Criminal immunities from computer offences for communications providers under TARs, TANs and TCNs remain broader than those applying to intelligence agencies for the same conduct.
- ✗ No requirement for the Attorney-General to give s 317S procedures for making TCN requests to IGIS, including any amendments to those procedures. *(This could be done administratively, but a statutory requirement would provide greater certainty that this would be done consistently.)*
- ✗ No requirement for ASIO's warrant reports to identify whether a TAR, TAN or TCN was used to request or compel a DCP to do a thing under a warrant.
- ✗ The exception in s 317ZH(4)(f) would allow ASIO to issue a TAN that 'gives effect to' one of its warrants by requiring the DCP doing an act or thing specified in the warrant is not explicitly limited to warrants that are in force at the time the TAN was issued (and not subsequently). *(This observation also applies to TARs and TANs issued by ASIO, TCNs issued for the benefit of ASIO, and TARs issued by ASIS and ASD, which request or require a DCP to provide assistance that gives effect to an authorisation obtained by the relevant agency.)*
- ✗ Ambiguity remains about whether TARs and TANs can cover the provision of repetitive assistance (doing the specified act multiple times) or whether a TAR or TAN is spent after a single instance of providing the specified assistance, and a new one would be needed.

- ***defences for IGIS officials; and***

Fully addressed in Government amendments

- ✓ Removal of evidential burden from IGIS officials in s 317ZF(5).
- ✓ Insertion of exception in s 63AC of the *TIA Act*.

- ***clear information sharing provisions.***

Fully addressed for IGIS in Government amendments

- ✓ Amendments to s 63AC of the *TIA Act*.

PJCIS recommendation 17

The Committee recommends that the Government:

- ***Amend clause 317ZG of Schedule 1 to explicitly prohibit an interception agency from asking a designated communications provider to voluntarily implement or build a systemic weakness or vulnerability under a technical assistance request;***

Fully implemented in Government amendments

✓ Section 317ZG applies to TARs (as well as TANs and TCNs).

- ***Amend clause 317ZH of Schedule 1 so that the 'general limits' on technical assistance notices and technical capability notices apply equally to technical assistance requests.***

Partially implemented in Government amendments (subject to one apparent technical issue)

✓ Subsection 317ZH(1) applies explicitly to TARs, in addition to TANs and TCNs.

× However, amendments to ss 317ZH(1) and (4) may be needed to account for the fact that ASD and ASIS can issue TARs. This appears to be a technical oversight. (Specifically, the *Intelligence Services Act* may need to be added to the list of Acts in paragraphs 317ZH(1)(a) and the exception in subsection 317ZH(4) may need to refer to giving help to ASD or ASIS under a TAR.)

Attachment C

Handling of IGIS concerns about Schedules 2 and 5 (ASIO Act)

The Committee's recommendations on the Bill, while inclusive, were directed to Schedule 1 (other than two discrete matters in recommendation 5 concerning disclosure provisions relevant to IGIS, which applied to provisions in Schedules 1, 2 and 5).

However, the Government moved some further amendments to address aspects of IGIS's concerns about Schedule 2 (ASIO warrants) and Schedule 5 (ASIO civil immunities for voluntary assistance, and compulsory assistance orders).

This attachment identifies those of IGIS's concerns that have been implemented in statute, and those that remain outstanding, as they have not been included in the Act or in the *ASIO Guidelines* at the time of writing. IGIS has not received advice from ASIO or the Department of Home Affairs about whether there is an intention to amend the Guidelines to include some or all of these matters.

IGIS concerns addressed in the Government amendments

Schedule 2 (extended powers under ASIO computer access warrants)

- ✓ **Reporting on post-warrant concealment:** Specific reporting requirements to the Attorney-General on post-warrant concealment activities (activities to conceal acts done under a warrant, and further concealment of those activities).
- ✓ **Equivalent safeguards for concealment activities as for computer access activities:** Concealment activities are subject to equivalent limitations on causing material interference, loss or damage to lawful computer users as those currently applying to computer access.

Schedule 5 (s 21A(1) civil immunities for voluntary assistance and s 34AAA assistance orders)

Civil immunities for voluntary assistance: s 21A(1)

- ✓ **Notification requirement:** Notification of IGIS of issuing s 21A(1) requests (civil immunities for voluntary assistance).
- ✓ **Form requirement:** Requirement that s 21A(1) requests must be made in writing, unless there are circumstances of urgency, or a risk of prejudice to security or operational security.

Compulsory assistance orders: s 34AAA

- ✓ **Previous requests:** ASIO's requests to the Attorney-General for the issuing of s 34AAA assistance orders must specify any previous requests made in relation to the person (and outcomes of those requests).
- ✓ **Integration with warrant reporting:** ASIO's warrant reports must include information about related s 34AAA assistance orders in relation to data obtained under the warrant.
- ✓ **Annual reporting:** ASIO's classified annual reports must include statistical information on 34AAA orders and s 21A(1) assistance requests.
- ✓ **Duty to advise Attorney-General if grounds for order have ceased to exist:** The Director-General of Security must inform the Attorney-General if satisfied the grounds for issuing an s 34AAA order have ceased to exist. The Attorney-General must revoke the order if satisfied that the issuing grounds have ceased to exist.

IGIS concerns not addressed

Schedule 2 (extended powers under ASIO computer access warrants)

- **Limitation on warrant reporting—temporary removals:** Warrant reports under s 34 are not required to specifically identify whether a computer or other thing has been removed from premises in all instances. (Reporting will only be required under existing provisions of section 34, if ASIO has assessed the removal to have caused material interference with the lawful use of the computer. This will make it difficult to oversee the exercise by ASIO of the new temporary removal powers, and its decision-making about whether a temporary removal caused a material interference.)

Schedule 5 (s 21A(1) civil immunities for voluntary assistance and s 34AAA assistance orders)

Civil immunities for voluntary assistance: s 21A(1)

- **Proportionality:** No statutory issuing criteria requiring the Director-General of Security (or delegate) to be satisfied that the conferral of civil immunity is reasonable and proportionate.
- **Exclusion of certain conduct causing serious loss or harm:** No statutory exclusion of conduct causing significant financial loss, or serious physical or mental harm to another person.
- **Maximum period of effect:** No statutory maximum period of effect for s 21A(1) requests. (Noting there is doubt that a period of effect could, in some way, be implied from separate legal instruments such as warrants or contracts.)
- **Overlap with Technical Assistance Notices:** No exclusion of conduct that could be the subject of a TAR under Part 15 of the *Telecommunications Act 1997* (inserted by Schedule 1 to the Act), noting that TARs are subject to stronger limitations than s 21A(1) voluntary assistance requests.
- **Conduct for which ASIO would require a warrant / authorisation to undertake directly:** No exclusion of conduct for which ASIO would require a warrant or an authorisation to carry out itself (except in those cases in which ASIO had already obtained a warrant or authorisation, which was in force at the time, and the person who is subject to an s 21A(1) request was also authorised to exercise authority under that warrant or authorisation).
- **Notification of IGIS if conduct causes serious harm or damage:** There is no requirement for ASIO to notify IGIS if it becomes aware that a person engages in conduct in purported reliance on a civil immunity under s 21A(1), and the act or thing exceeds applicable limits on the immunity (including the additional limits IGIS has suggested). For example, if the conduct causes another person to suffer significant financial loss, property loss or damage, or physical or mental harm.
- **Powers of variation and revocation:** No specific statutory power of variation or revocation. (Noting that s 33(3) of the *Acts Interpretation Act 1901* would not be available, at least for oral requests; and there is legal uncertainty about the existence and scope of implied powers of variation or revocation.)
- **Repetitive provision of assistance:** Ambiguity as to whether requests can cover the repetitive provision of assistance, or are spent after the first performance of the specified conduct. (Proportionality requirements and a maximum period of effect will be even more important if requests are intended to cover, and therefore confer immunity for, the repetitive provision of assistance.)

Compulsory assistance orders: s 34AAA

- **Persons who may be subject to an order:** Assistance orders can be issued in relation to any person who is reasonably suspected of being involved in an activity that is prejudicial to security. This is not required to be an activity that is prejudicial to the security matter in respect of which the underlying warrant is issued, and could be any unrelated security matter. (IGIS is aware that the Department of Home Affairs gave evidence to the PJCIS that this broader application was not the intent.)
- **Not all orders are required to specify essential matters:** Assistance orders are only required to specify essential matters (including the compliance period, place of attendance and conditions on the order) if a computer has been removed from premises under a warrant. This means that, where a computer is accessed wholly remotely (for example, under ASIO's computer access warrants) there is no requirement for orders to include these conditions. This reduces transparency in the terms of an order that the Attorney-General is being asked to approve, and in the information given to persons who are subject to orders, because these matters are not required to be recorded explicitly on the face of the order itself.
- **Arbitrary deprivation of liberty:** No statutory safeguards against the risk of orders requiring a person to attend a place to provide assistance resulting in an arbitrary deprivation of liberty.
- **Retention / deletion of information obtained under an assistance order:** 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 under the *ASIO Act*. (Such an obligation exists in section 31 in relation to information obtained under the underlying special powers warrant. Not all information obtained under an s 34AAA warrant will be covered by s 31 itself. For example, login credentials to a computer, potentially including biometric identification information.)
- **Cessation of action taken under an order where issuing grounds no longer exist:** No obligation on the Director-General of Security to take all necessary steps to cease executing an s 34AAA order if satisfied that the issuing grounds have ceased to exist, noting that such an obligation applies to ASIO's special powers warrants under s 30(1)(b).
- **Notification and service of orders:** No statutory requirements for the notification and service of assistance orders on persons.
- **Interaction with ASIO's questioning and detention warrants:** No statutory guidance on the execution of an assistance order in relation to a person who is the subject of an ASIO questioning warrant or a questioning and detention warrant (including a role for IGIS, where in attendance for the compulsory questioning of a person).

UNCLASSIFIED

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Correspondence ref: OIGIS/OUT/2018/193 File ref: 2018/140

Mr Andrew Hastie MP
Chair
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

Dear Chair

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

I enclose a further supplementary submission to the Committee's review of the above Act.

This supplementary submission responds to comments made in submission 16.1 of the Department of Home Affairs, in relation to the matters raised in IGIS submission 1.1. This document was also provided to the Committee as background information on 12 February 2019, in connection with a private briefing. I confirm that the submission is unclassified and able to be published on the Committee's website.

Thank you for the opportunity to contribute to this review. IGIS would be pleased to assist the Committee further as required.

Yours sincerely

[redacted]

Jake Blight
Acting Inspector-General

13 February 2018

Inspector-General of Intelligence and Security: Responses to Home Affairs supplementary submission 16.1

Schedule 1—industry assistance scheme: TARs (ASIO, ASD, ASIS); TANs (ASIO); and TCNs (requested by, or for the benefit of, ASIO)

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
1.	**No annual reporting by ASIS and ASD (TARs)** This could be done administratively. However, IGIS has not been advised of any commitment to do so. ***IGIS submission 1.1, p. 6.***	ASD and ASIS can (at their discretion) report these matters in their classified annual reports given under the *ISA*. It would be open to the Finance Minister to issue a direction under s 105D of the *PGPA Act.* ***Home Affairs submission 16.1, Attachment B, p. 1.***	In the course of commenting on draft Government amendments, in December 2018, IGIS indicated to the Department the possibility of making an administrative commitment to include annual reporting on TARs as part of the requirements for the classified annual reports of ASD and ASIS. (This included the potential for the issuing of Finance Minister's directions under the *PGPA Act*). However, IGIS has not been notified of any such commitment, and the Department's comments re-state the existence of administrative discretion. It may be desirable to consider a consistent approach to the way in which annual reporting obligations are imposed on ASD, ASIS and ASIO (noting ASIO is subject to express statutory reporting requirements.) This would mean that the reporting obligations for all agencies that are eligible to use the industry assistance scheme are equally transparent. ***See: IGIS submission 52, p. 38.***
2.	**Notification of harmful acts done in reliance, or purported reliance, on immunities** No notification of IGIS by ASIO, ASIS or ASD if a provider does an act under a TAR, TAN or TCN in reliance or purported reliance on the civil or criminal immunity that causes significant loss, damage, injury or interference with lawful computer use (and annual reporting of statistical information about these instances, on a classified basis if necessary). ***IGIS submission 1.1, p. 6.***	The Department has recommended to ASIO, ASIS and ASD that these matters are addressed in their classified annual reports. ***Home Affairs submission 16.1, Attachment B, p. 1.***	The key suggestion by IGIS was for ***'per incident' notification to IGIS***, and not merely statistical annual reporting. 'Per incident' notification would facilitate the prompt identification of matters to IGIS, and consequently the timely identification of any issues in the agency's management of the power to confer immunity on the DCP, before there is a need for major remedial action. Such a notification requirement could facilitate best practice by intelligence agencies in having systems and processes in place to monitor acts done by DCPs in reliance on the immunities conferred, to ensure that they remain proportionate. While annual reporting will assist with *ex post facto* oversight of the agencies' actions across multiple TARs, TANs or TCNs at 12 monthly intervals, 'per incident' notification will enable timely and detailed oversight of individual incidents in which immunities are enlivened. ***See: IGIS submission 52, pp.30,33,38.***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
3.	**Issuing criteria: limited consideration of third party impacts** No express requirement for persons issuing TARs, TANs and TCNs (as applicable) to consider the potential impacts of an immunity on all third parties who may be affected by the DCP's actions under the request or notice; only the those persons who are not of interest to ASIO (in relation to TARs, TANs and TCNs) or ASIS or ASD (in relation to TARs). ***IGIS submission 1.1, p. 7.***	The Department considers that the existing decision-making criteria 'directly address a wide range of considerations that go to the impact of a TAN, TAR or TCN on third parties'. The Department also sought to bring to the Committee's attention 'the fact that IGIS may be referring to the Explanatory Document released in connection with an exposure draft of the legislation rather than the Explanatory Memorandum' to the Bill as introduced, in support of the statement in IGIS's submission that 'IGIS concurs with the statement in the Explanatory Memorandum that the concepts of reasonableness and propriety would require consideration of this matter in each case'. ***Home Affairs submission 16.1, Attachment B, p. 2.***	Home Affairs' response misunderstands the suggestion made by IGIS in our submissions and evidence to the PJCIS on the Bill (and restated in our submission on the review of the Act). The Government amendments to the Bill partially implemented IGIS's suggestion for there to be an express issuing criterion for TARs, TANs and TCNs, which required consideration of the impacts of the immunity on third parties whose rights to legal remedies against the DCP may be extinguished. The Government amendments are limited to consideration of impacts on persons who are **not of interest** to ASIO, ASD or ASIS: ss 317ZJA; 317RA, 317ZAA. There is no requirement to consider the impacts on persons who **are of interest** to these agencies. (Such a requirement may now be impliedly excluded by the presence of an express requirement to consider impacts on persons who are not of interest to the agencies). It is unclear why the amendments are limited in this way, especially given that persons who are of interest to an intelligence agency may ultimately be eliminated as an investigative target; or may be unknowingly or unwittingly involved in prejudicial activities (for example, as a conduit through which someone else is acting). In our submission to the Bill, IGIS concurred with the statement in the EM to the Bill that, in the form in which the provisions were introduced, ***'the decision-maker must also consider wider public interest, such as any impact on … third parties'*** (EM, p. 149 at paragraph 132, as cited directly in IGIS's submission). However, as noted above, the presence in the Act of a more limited requirement to only consider impacts on some third parties may mean that this result can no longer be implied. ***See: IGIS submission 52, p. 19.***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
4.	**No fixed maximum period of effect for TARs** 90-day maximum in s 317HA(1) applies only if the TAR does not specify an expiry date. There is no limit on the expiry date that can be specified. ***IGIS submission 1.1, p. 7.***	The Department refers to unattributed advice that a maximum period of effect is unworkable. There is an intention for TARs to be used to deploy capabilities over long period, and this is appropriate given the voluntary nature of TARs. The period of time will need to be considered on a case-by-case basis. ***Home Affairs submission 16.1, Attachment B, p. 3.***	It is unclear from the unattributed advice referred to by the Department why it would be unworkable to have a maximum period of **any duration** (and with there being no limit on the number of times a TAR may be re-issued). ***Inconsistency with other powers to confer immunities*** IGIS notes that other authorisation-based powers conferred on ASIO, ASD and ASIS are intended to support operations that run over a long period of time, but they have a maximum duration and can be 'renewed' (by being re-issued) multiple times. For example, ASIO's special intelligence operations (SIOs) are subject to a maximum period of effect of 12 months. Most ministerial authorisations (MA) issued to ASIS and ASD under the *ISA* are subject to a maximum period of effect of six months. (Notably, civil and criminal immunities also attach to acts done as part of an SIO, or under an MA in the proper performance of the functions of the intelligence agency.) The operations to which these authorisations relate can run for many years. ***Benefits of a statutory maximum period of effect*** As IGIS noted in our evidence to the PJCIS review of the Bill, a major benefit of a statutory maximum period of effect is that it creates a mechanism for the periodic review of the continuing necessity and proportionality of immunities from criminal and civil liability conferred by an agency head. In this respect, the power of the heads of ASIO, ASIS and ASD to confer immunities under TARs is **more expansive** than powers effectively conferred on Ministers via the authorisation of SIOs and the issuing of MAs that enliven statutory immunities under the *ASIO Act* and *ISA*. ***Alternative to an express periodic review requirement for TARs*** If no maximum period of effect is prescribed for TARs, then IGIS suggests, in the alternative, an express periodic review requirement, in either the *Telecommunications Act* or in Ministerial Guidelines to the relevant intelligence agencies. ***See: IGIS submission 52, pp. 23-24.***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
5.	**Overlap of TARs with ASIO s 21A(1) requests** No statutory clarification of overlap between TARs and ASIO s 21A(1) requests. ***IGIS submission 1.1, p. 7.***	The Department considers the distinction to be 'clear on the face of the legislation' and it 'remains unclear what the benefit of further drawing out this distinction may be, particularly because they are voluntary powers that will be utilised distinctly and to the awareness of the IGIS and the relevant person'. ***Home Affairs submission 16.1, Attachment B, p. 3.***	The subjective policy intention identified by the Department is not given effect in the provisions of the *Telecommunications Act* or the *ASIO Act*. Although the stated intention may be that TARs and s 21A(1) requests will not be used interchangeably, they are legally capable of being used in this way, in the absence of any prohibition. As IGIS noted in our submissions to the PJCIS review of the Bill, this raises a propriety risk, given that both forms of immunity can cover the same conduct, but are subject to different safeguards, conditions and limitations. If there is no intention for ASIO's s 21A(1) notices to be used in place of TARs (or vice versa) then giving express legal effect to this intent would provide an important safeguard against the new powers to confer civil immunities being used in a manner that is contrary to the stated policy intention. ***See: IGIS submission 52, pp. 7, 55-56; submission 52.1, pp.10-11.***
6.	**Limitations on harmful conduct** No further limitations on civil immunities (exclusion of conduct causing serious financial loss, damage to property, personal injury or harm, or an offence). ***IGIS submission 1.1, p. 7.***	Such limitations 'would, in the Department's view, limit the utility of the industry assistance scheme'. The Department also states that, 'it is highly unlikely' that conduct causing such results could be capable of authorisation under the issuing criteria of reasonableness and proportionality. ***Home Affairs submission 16.1, Attachment B, p. 3.***	The two propositions advanced by the Department appear to be contradictory. It is not clear how excluding certain forms of harmful conduct from the immunity could simultaneously: limit the utility of the industry assistance scheme; **and** be unnecessary because the issuing criteria would operate to prevent the conferral of immunities that would cause these forms of harm. If there is an intention for the industry assistance scheme to be capable of immunising such harmful conduct, IGIS notes that this would be a highly significant devolution of power to agencies. It would confer on agency heads a wider power to grant immunity than the Attorney-General can confer by authorising an SIO (noting that the SIO scheme expressly excludes conduct causing serious injury, and loss of or damage to property). TARs and TANs purporting to confer immunities of this kind would require close oversight; and in particular close oversight of agencies' monitoring and controls over the DCP's activities that may cause these forms of harm. This makes IGIS's suggestion above for 'per incident' notification of acts that invoke the immunity even more important. ***See: IGIS sub 52, pp. 29, 53-54.***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
7.	**Criminal immunities: computer offences** Criminal immunities from computer offences for communications providers under TARs, TANs and TCNs remain broader than those applying to intelligence agencies for the same conduct. ***IGIS submission 1.1, p. 7.***	The Department's comments appear to confirm that it is the intention for DCPs to be conferred with broader immunities from criminal liability to computer offences than equivalent immunities which are available to members of ASIO, ASD and ASIS in the proper performance of their functions. ***Home Affairs submission 16.1, Attachment B, p. 4.***	IGIS remains concerned about propriety risks that arise from the effective conferral of power on intelligence agency heads to grant DCPs broader immunities from criminal liability than are available to intelligence agency members. In particular: • A DCP would appear to have effective criminal immunity if a TAR or TAN has no legal effect because it contravenes the prohibition in s 317ZH(1) on assistance for which the agency would require a warrant or authorisation, and an exception in s 317ZH(4) did not apply (for example, s 317ZH(4)(f) did not apply as there was no extant warrant or authorisation). • A DCP would not be subject to the equivalent limitations that apply to immunities for intelligence agency members. For example, in the case of ASIO, a requirement that material interference with the lawful use of a computer is only permitted where ***necessary*** to access relevant data under a warrant. In the case of ASIS and ASD, the immunity is limited to acts done in the ***proper*** performance of those agencies' functions. If the intention is for DCPs to have a broader immunity, then the propriety of agencies' decision-making to effectively confer that immunity by issuing TARs or TANs will require close attention by IGIS. It will also be necessary for IGIS to pay close attention to agencies' systems and practices for monitoring DCPs' activities under TANs and TARs to ensure that the immunity remains reasonable and proportionate after it has been issued (and varied or revoked if it is not). This will make it even more important for IGIS to receive 'per incident' notifications of instances in which a DCP engages the criminal immunity, and there is resultant loss, harm, interference or damage to third parties (as per the suggestion noted at comment no. 2 above). ***See: IGIS submission 52, p. 31-33.***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
8.	**Copies of AG's TCN procedures to IGIS** No requirement for the Attorney-General to give s 317S procedures for making TCN requests to IGIS, including any amendments to those procedures. (This could be done administratively, but a statutory requirement would provide greater certainty that this would be done consistently.) ***IGIS submission 1.1, p. 7.***	The Department suggests that IGIS 'has significant powers to review any such procedures under their inspection function' and to oversee ASIO's compliance, under s 9A of the *IGIS Act.* The Department also comments that, as TCNs may be requested by agencies outside IGIS's remit, 'jurisdictional considerations must be taken into account. ***Home Affairs submission 16.1, Attachment B, p. 5.***	The Department's comments appear to misunderstand IGIS's suggestion; and demonstrate a limited understanding of the way in which independent operational oversight is conducted. IGIS is seeking a requirement for the Attorney-General to give the IGIS a copy of the s 317S procedures when they are made, and when they are changed. This will ensure that IGIS has reliable access to the current version of the procedures, in order to oversee ASIO's compliance with them in requesting TCNs. This suggestion would simply bring IGIS's ability to access s 317S procedures into line with the broad range of existing provisions of intelligence legislation that require copies of applicable rules and guidelines to be given to IGIS. (For example requirements under the *ISA* and *ONI Act* to give IGIS copies of privacy rules; requirements under the *ISA* to give IGIS copies of guidelines and authorisations for the use of force by ASIS; and requirements under the *ASIO Act* to give IGIS copies of Ministerial guidelines.) The obligation would be on the Attorney-General, **not** the Home Affairs Minister, his Department or ASIO. IGIS has not received any indication from the Attorney-General or his portfolio that there would be any objection to such a requirement. IGIS's suggestion is **not** about IGIS attempting to conduct a review of the substance of the Attorney-General's procedures (noting limitations in s 9AA of the *IGIS Act* on inquiring into Ministers' actions). Nor is it an attempt to oversee any other agency's compliance with those procedures (noting limitations on IGIS functions in s 8 of the *IGIS Act*). Rather, the suggestion would simply provide a stronger assurance that IGIS will have the most up-to-date version of the procedures (and is familiar with them) when overseeing ASIO's compliance in making TCN requests. It will avoid the impost on ASIO that would otherwise arise, as IGIS would need to request ASIO to provide advice, ***in relation to every TCN request***, about the current version of the s 317S procedures. ***See: IGIS submission 52, p. 33-34.***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
9.	**Warrant reports: identification of related TARs, TANs and TCNs** No requirement for ASIO's warrant reports to identify whether a TAR, TAN or TCN was used to request or compel a DCP to do a thing under a warrant. ***IGIS submission 1.1, p. 7.***	The Department suggests that such information 'could be obtained by IGIS through their general inspection function or the multiple legislative pathways for oversight provided by the Act'. ***Home Affairs submission 16.1, Attachment B, p. 5.***	The Department's comment appears to demonstrate a limited practical understanding about how IGIS conducts independent operational oversight of intelligence agencies. As noted in IGIS's submissions on the Bill, there is now the potential for intelligence operations to utilise multiple, interrelated sources of authority (for example, TARs, TANs, TCNs and special powers warrants). However, the connection between each power used in a particular operation may not be evident on the face of the individual instruments inspected by IGIS (eg, the warrant instrument or the TAR, TAN or TCN document). If there was no mechanism requiring the identification of that connection as a matter of routine, it would be necessary for IGIS officials to undertake a detailed, forensic exercise in searching ASIO's records (and requesting information from ASIO) to ascertain ***whether*** such a connection existed in each and every inspection. This would be highly inefficient, and would divert limited resources away from substantive oversight of matters of legality and propriety. It is preferable that there is a clear, standing requirement for ASIO to identify these connections in its reports on relevant special powers warrants, which would then form a basis for targeted searches and analysis by IGIS officials during inspections. ***See: IGIS submission 52, p 11.***
10.	**Ambiguity in provisions authorising TARs, TANs and TCNS to 'give effect' to warrants** The exception in s 317ZH(4)(f) would allow ASIO to issue a TAR or TAN (or request a TCN) that 'gives effect to' one of its warrants by requiring the DCP doing an act or thing specified in the warrant is not explicitly limited to warrants that are in force at the time the TAR/TAN/TCN was issued (and not subsequently). ***IGIS submission 1.1, p. 7***	The Department suggests that the words in s 317ZH(4)(e) *'assist in, or facilitate in, giving effect to a warrant'* make clear that the provision 'is not about discharging authority within the warrant itself but rather undertaking activities that support what is being authorised by a warrant. Accordingly, a provider cannot be asked to do a thing that would require authorisation under a warrant itself'. ***Home Affairs submission 16.1, Attachment B, p. 5.***	The Department's comments appear to be inaccurate. The Department refers to the exception in s 317ZH(4)(e). However, IGIS's comments were directed to the ***separate exception in s 317ZH(4)(f)***, which covers the provision of assistance for the purpose of 'giving effect to a warrant' and not merely assisting or facilitating in doing so (which is covered separately in s 317ZH(4)(e)). The ordinary meaning of the words 'giving effect' to a warrant (in the context of a set of provisions that ***separately*** address assistance or facilitation) would appear to cover the doing an act or thing that is authorised under the warrant. ***[Continued]***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
			Officers from the Department met with IGIS officials on 27 November 2018 to discuss IGIS's concerns about the Bill. IGIS asked the Departmental officers about the intended meaning of s 317ZH(4)(f). We were advised that the provision ***was intended*** to cover the doing an act or thing authorised under a warrant, but ***only*** an extant warrant. (That is, not a warrant that was issued or came into force after the issuing of the TAN or TCN.) If that intention has changed since the passage and commencement of the Act, then IGIS suggests that the meaning of s 317ZH(4)(f) is ambiguous and should be clarified; or the provision simply removed and sole reliance placed on the 'assistance and facilitation' exception in s 317ZH(4)(e). ***See: IGIS submission 52, pp. 9-12.***
11.	**Repetitive provision of assistance** Ambiguity remains about whether TARs and TANs can cover the provision of repetitive assistance (doing the specified act multiple times) or whether a TAR or TAN is spent after a single instance of providing the specified assistance, and a new one would be needed. ***IGIS submission 1.1, p. 7.***	The Department has confirmed that TARs and TANs are intended to authorise the provision of repetitive assistance. The Department also suggests that the concerns raised by IGIS are in some way alleviated by the existence of a maximum period of effect for TANs. ***Home Affairs submission 16.1, Attachment B, pp. 5-6.***	As noted in previous evidence to the Committee in the review of the Bill, IGIS is **not suggesting** an amendment to provide that a notice or request is spent after the provision of a single act of assistance. Rather, IGIS is suggesting an amendment to clarify the intended application, and thereby remove the ambiguity that currently exists in the provisions. The Department has indicated that TARs, TANs and TCNs should be capable of authorising repetitive acts. Consequently, the assessment of proportionality of requests and notice covering repetitive acts will be particularly important. (This is especially important for those forms of assistance that are not subject to a maximum period of effect, namely TARs; but proportionality is important in ***all cases***). IGIS remains of the view that the *ASIO Minister's Guidelines* should be updated to provide ***specific guidance*** on the assessment of proportionality in the exercise of powers to confer immunities from legal liability. (This would be ***additional to*** the general guidance in existing paragraph 10.4 about proportionality in the collection of information in inquiries and investigations.) ***See: IGIS submission 52, p. 25.***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
12.	**Technical issue: limits on TARs, TANs, TCNs** Amendments to ss 317ZH(1) and (4) may be needed to account for the fact that ASD and ASIS can issue TARs. This appears to be a technical oversight. (Specifically, the ISA may need to be added to the list of Acts in paragraphs 317ZH(1)(a)-(f) and the exception in subsection 317ZH(4) may need to refer to giving help to ASD or ASIS under a TAR.) ***IGIS submission 1.1, p. 8.***	The Department states that the reference in s 317ZH(1)(f) to another law of the Commonwealth is sufficient to cover Ministerial authorisations under the *ISA* (being a form of authorisation that is 'additional to those available in the most relevant Acts' that are identified in the other paragraphs of s 317ZH(1)). The Department appears to acknowledge the need for a correction to the exception in s 317ZH(4). ***Home Affairs submission 16.1, Attachment B, p. 6***	***Express recognition of the ISA in the s 317ZH(1) prohibition*** IGIS suggests that s 317ZH(1) should be amended to expressly identify Ministerial authorisations under the *ISA* in the prohibition established under that subsection. The Department has indicated the intention is for s 317ZH(1) to list 'the most relevant Acts' that confer authorisation requirements on agencies authorised to issue TARs (as well as TANs and requesting TCNs). The *ISA* is the core piece of legislation imposing authorisation requirements on ASIS and ASD (which are two of the three intelligence agencies authorised to issue TARs) ***Inclusion of ASD and ASIS in the s 317ZH(4) exception*** IGIS notes that s 317ZH(4) would need amendment to include ASD and ASIS in the exception to the prohibition in s 317ZH(1), unless there is an intention for that prohibition to be absolute in the case of ASIS and ASD (which would be in contrast to the availability of exceptions for ASIO and law enforcement agencies). It appears from the Department's comments that this is an unintended omission, rather than a deliberate policy intention.

Schedule 2—ASIO computer access warrants (extended powers, including temporary removal and telecommunications interception)

[Note: blue rows denote key outstanding concerns identified in IGIS submission 1.1]

No.	IGIS suggestion ***(in submission 1.1, summarised from previous submissions and evidence)***	Summary of Home Affairs comment ***(from submission 16.1, Attachment B)***	IGIS further comments
13.	**Limitation on warrant reporting: temporary removals (ASIO Act, s 34)** Warrant reports under s 34 are not required to specifically identify whether a computer or other thing has been removed from premises in all instances. Reporting will only be required under existing provisions of section 34, if ASIO has assessed the removal to have caused material interference with the lawful use of the computer. This will make it difficult to oversee the exercise by ASIO of the new temporary removal powers, and its decision-making about whether a temporary removal caused a material interference. ***See: IGIS submission 1.1, pp. 4 and 10.***	'At present, section 34(2) requires the a warrant report to include details of anything done that materially interfere, interrupt or obstruct the lawful use by other persons of a computer or other electronic equipment, or a data storage device. The IGIS has overarching authority to seek information about the use and reasonableness of ASIO powers, including these relevant provisions and associated decision-making processes. Agencies are committed to engaging constructively with the IGIS to provide the necessary information on a case-by-case basis. These reporting requirements, combined with IGIS significant overarching inspection powers, are sufficiently robust.' ***See: HA submission 16.1, Attachment B, p. 6.***	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. As noted in our submission on the Bill, 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.) This may lead to inconsistent interpretations, and therefore inconsistent reporting practices by ASIO. • The absence of a specific reporting requirement for all removals may also mean that that suitably detailed records may not be made (or may not be made consistently) of the reasons for, and duration of, each removal, which would make oversight even more difficult. Further, the expectation conveyed by Home Affairs that IGIS must rely exclusively on the standing inspection function in s 9A of the *IGIS Act* to obtain this information on a case-by-case basis would result in significant inefficiency in oversight. IGIS uses ASIO's warrant reports as a basis for focusing our inspections of those warrants. If there were no reporting requirement, IGIS would separately ask ASIO, for ***each and every computer access warrant***, to provide information whether a computer or other thing was removed from those premises, so that IGIS could then examine those activities (including ASIO's decision-making about whether each removal caused a material interference). ***See: IGIS submission 52, AA Bill, pp. 45-46.***

Schedule 5—ASIO s 21A(1) requests (new power to confer civil immunities on persons voluntarily assisting ASIO)

[Note: blue rows denote key outstanding concerns identified in IGIS submission 1.1]

No.	IGIS suggestion ***(in submission 1.1, summarised from previous submissions and evidence)***	Summary of Home Affairs comment ***(from submission 16.1, Attachment B)***	IGIS further comments ***(references are to IGIS submissions on the Bill)***
14.	**No proportionality assessment** The Director-General of Security (or delegate) is not required by the Act to be satisfied that the conferral of civil immunity is reasonable and proportionate, as a precondition to granting the immunity. (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.) ***See: IGIS submission 1.1, pp. 3, 10.***	The Department suggests that a specific proportionality requirement in the issuing criteria for s 21A(1) requests is unnecessary in view of the existing proportionality requirement in the Minister's Guidelines to ASIO (paragraph 10.4). ***Home Affairs submission 16.1, Attachment B, pp. 6-7.***	As IGIS explained in detail in our submissions and evidence to the PJCIS on the Bill, our concern is the absence of ***specific guidance*** on the requirements of proportionality in relation to the exercise of a power to confer a civil immunity from liability. While the existing *Guidelines* contain a proportionality requirement, it is directed generally to the collection of information in investigations and inquiries. IGIS supports the inclusion of ***additional, specific guidance*** on the application of proportionality to the new power to confer civil immunities. IGIS has also noted that the inclusion of a specific proportionality requirement in the issuing conditions for s 21A(1) immunities would have significant benefits for compliance and oversight. In particular, promoting consistency of decision-making and good practice in record-keeping of decision-making in relation to specific statutory criteria. (Relevantly, IGIS's *2017-18 Annual Report* reported that IGIS had identified widespread deficiencies in ASIO's record keeping across all areas inspected.) ***See: IGIS submission 52, p. 17-18 and 53.***
15.	**No exclusion of certain harmful conduct** The immunity is not subject to an exclusion for conduct causing significant financial loss, or serious physical or mental harm to a person. (The exclusions in s 21A(1) apply only to significant loss of or damage to property, and conduct involving the commission of an offence.) ***See: IGIS submission 1.1, pp. 4, 10.***	The Department states that 'the policy intention is to cover pure economic loss and conduct resulting in physical or mental harm or injury within the immunity'. It states that such coverage is 'consistent with … the current operation of similar powers such as section 35K of the *ASIO Act*'. ***Home Affairs, submission 16.1, Attachment B, p. 7.***	If the policy intention is for the Director-General or delegate to have the power to confer an immunity on persons, in relation to acts that cause serious financial loss and serious physical or mental harm or injury, then IGIS considers that our suggestions for an express proportionality requirement and a maximum period of effect becomes even more important. Further, the Department's suggestion that the scope of the s 21A(1) immunity is 'consistent with' existing immunities is inaccurate. For example, the Attorney-General's power to authorise special intelligence operations (and therefore confer immunity) expressly excludes conduct that causes (among other things) death or serious personal injury. ***[Continued]***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
			In addition, to the scope of SIO-related immunities being more limited, the authorisation requirements for the conferral of civil immunity under an SIO are more onerous than those applying to the conferral of an s 21A(1) immunity. (For example, SIOs can only be approved in relation to a sub-set of ASIO's functions, and there are express proportionality requirements in the authorisation criteria.) The result is that s 21A(1) would empower the Director-General (or delegate) to confer a broader civil immunity than the Attorney-General could under the SIO regime, with fewer issuing conditions and limitations. ***See: IGIS submission 52, pp. 29, 51-54; IGIS submission 52.1, p. 11.***
16.	**No maximum period of effect** Requests for voluntary assistance, and consequently the civil immunity, are not subject to any maximum period of effect. ***See: IGIS submission 1.1, pp. 4, 10.***	The Department considers that a maximum period of effect is 'unnecessary' in view of the 'broad conduct that the civil immunity is intended to cover'. ***Home Affairs submission 16.1, Attachment B, p. 7.***	IGIS remains of the view that a maximum period of effect (with the ability to re-issue requests) is an important safeguard. It creates a mechanism for the review of whether an immunity remains necessary and proportionate. IGIS considers that the breadth of the conduct that the civil immunity is intended to cover makes it more important, not less important, that there is a statutory maximum. As noted above, other authorisations for intelligence operations that are intended to continue for an extended period of time are nonetheless subject to maximum periods of effect, with the ability to obtain an unlimited number of new authorisations. (For example, SIOs and most Ministerial authorisations under the ISA, both of which enliven applicable immunities, are subject to maximum periods of effect.) If there is no intention to apply a statutory maximum period of effect then IGIS would support, in the alternative, an ***express requirement*** for the Director-General or delegate to periodically review the appropriateness of the immunity; and an obligation to vary or revoke the request if satisfied it is no longer reasonable or proportionate. ***See: IGIS submission 52, p. 56; IGIS submission 52.1, p. 11.***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
17.	**Overlap with TARs** No exclusion of conduct that could be the subject of a TAR under Part 15 of the Telecommunications Act 1997 (inserted by Schedule 1 to the Act), noting that TARs are subject to stronger limitations than s 21A(1) voluntary assistance requests. ***See: IGIS submission 1.1, p. 10.***	The Department acknowledges that 'there may be instances of assistance that could be addressed by the use of either powers' (that is an s 21A(1) request or a TAR). The Department appears to suggest that statutory clarification is unnecessary because TARs are intended to be used as part of a broader industry assistance framework. ***Home Affairs, submission 16.1, Attachment B, p. 7.***	As noted above in relation to TARs, the statement of subjective policy intent about the interaction of TARs and s 21A(1) requests is not given effect in the provisions of the *Telecommunications Act* or *ASIO Act.* It is therefore legally possible for s 21A(1) to be used other than as intended (that is, by covering conduct that could be the subject of a TAR). IGIS remains concerned by the propriety risk that exists, due to the two sets of powers each being able to confer immunity for the same conduct, but subject to differences in issuing conditions, limitations and other safeguards. (In particular, even the limited exclusions from conduct covered by the immunity conferred by TARs do not apply to s 21A(1) requests.) Since the policy intention is for s 21A(1) requests not to be used in substitution for TARS, then giving this express statutory effect would remove any risk of use contrary to that intent. ***See: IGIS submission 52, p. 56; IGIS submission 52.1, pp. 10-11.***
18.	**Actions for which ASIO would require a warrant or authorisation to do directly** No exclusion of conduct for which ASIO would require a warrant or an authorisation to carry out itself (except in those cases in which ASIO had already obtained a warrant or authorisation, which was in force at the time, and the person who is subject to an s 21A(1) request was also authorised to exercise authority under that warrant or authorisation). ***See: IGIS submission 1.1, p. 10.***	The Department appears to suggest there is an intention for ASIO exercise the power to confer civil immunities under s 21A(1) on persons outside the Organisation (such as human sources) in respect of activities for which ASIO would require a warrant to do itself (such as searching premises). The Department suggests that inserting a statutory prohibition on using s 21A(1) in these circumstances would 'prohibit ASIO from gathering essential intelligence' or would 'force ASIO to utilise more intrusive powers to achieve outcomes ordinarily done through voluntary means'. ***Home Affairs submission 16.1, Attachment B, p. 8.***	The Department's comments appear to misunderstand IGIS's concerns. The issue IGIS has raised is the creation of a potential propriety risk that s 21A(1) requests could be used in place of existing activities that ASIO undertakes under a warrant. In particular, while there is presently no prohibition on using human sources to do acts or things that do not constitute an offence by those persons (but would if ASIO undertook them directly), there is also presently no power to confer a civil immunity on those human sources (except under an SIO). That is, a human source may presently be unable to undertake some activities because they would attract civil liability, even though they would commit no criminal offence. It is the conferral of a significant new power on ASIO to grant a civil immunity to human sources (and others) that creates the propriety risk that s 21A(1) could be used in place of warrants; and potentially also in place of foreign intelligence authorisations under s 27B. IGIS considers that, as a minimum, propriety considerations should be addressed in the *Minister's Guidelines*.

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
			If there is no intention to exclude from the power in s 21A(1) conduct for which ASIO would require a warrant to undertake itself, then IGIS will oversee the propriety of ASIO's decision-making in selecting the relevant form of legal authority in particular operations. That would include oversight of compliance with applicable requirements in the *ASIO Guidelines*, if amended. ***See: IGIS submission 52, pp. 54-55.***
19.	**Notification of IGIS if conduct causes serious harm or damage** There is no requirement for ASIO to notify IGIS if it becomes aware that a person engages in conduct in purported reliance on a civil immunity under s 21A(1), and the act or thing exceeds applicable limits on the immunity (including the additional limits IGIS has suggested). For example, if the conduct causes another person to suffer significant financial loss, property loss or damage, or physical or mental harm. ***See: IGIS submission 1.1, p. 10.***	The Department states that 'existing oversight mechanisms sufficiently permit oversight of this aspect of the regime'. ***Home Affairs submission 16.1, Attachment B, p. 9.***	See **comment no 2 above**, which responded to the same comments from the Department on IGIS's suggestion for equivalent notification requirements for TARs, TANs and TCNs. 'Per incident' notification would facilitate the prompt identification of matters to IGIS, and consequently the timely identification of any issues in the agency's management of the power to confer immunity on a person, before there is a need for major remedial action. Such a notification requirement could facilitate best practice by intelligence agencies in having systems and processes in place to monitor acts done by persons subject to s 21A(1) requests in reliance on the immunities conferred, to ensure that they remain proportionate. ***See: IGIS submission 52, pp. 30, 33, 38; IGIS submission 52.1, pp. 12-13.***
20.	**Powers of variation and revocation** No specific statutory power of variation or revocation. (Noting that s 33(3) of the *Acts Interpretation Act 1901* would not be available, at least for oral requests; and there is legal uncertainty about the existence and scope of implied powers of variation or revocation.) ***See: IGIS submission 1.1, p. 10.***	The Department asserts that the power or revocation and variation in s 33 of the *Acts Interpretation Act* (which applies to 'instruments of a legislative or administrative character') applies to s 21A(1) requests. ***Home Affairs submission 16.1, Attachment B, p. 9.***	As noted in IGIS's submissions on the Bill, there is ambiguity about whether s 33(3) of the *Acts Interpretation Act* (*AIA*) applies to s 21A(1). (Noting that oral requests are evidently not 'instruments' that could enliven the rule in s 33(3). There is also ambiguity as to whether a power to make a request, with a written form requirement, amounts to a power to make an 'instrument' for the purpose of s 33(3) of the *AIA;* or whether it is merely a requirement to record decisions in writing, as a matter of good administrative practice. Courts have distinguished between these two concepts in interpreting s 33(3) of the *AIA,* and have held that the rule in s 33(3) ***does not apply*** to provisions of the latter kind.) ***[Continued]***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1, Attachment B)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
			IGIS suggests that, given the significance of a power to confer immunities from legal liability, it is preferable that the source and scope of powers of variation and revocation is placed beyond any doubt (consistent with provisions governing the variation and revocation of TARs, TANs and TCNs; and other provisions governing variations to, and revocations of, authorisations issued to ASIO, including warrants and SIOs.) IGIS suggests that the need for certainty is particularly important given inconsistencies in the Department's explanations to the PJCIS of the intended source of legal authority (which has been variously described in the Department's supplementary submissions on the Bill as being s 33(3) of the *AIA,* and an implied power from the provisions of s 21A(1) itself). This inconsistency supports the inclusion of an express provision that places the source and scope of authority beyond doubt, so that problems do not arise latently when powers are exercised. This will make both compliance and oversight more effective. ***See: IGIS sub 52, pp. 36 and 58; IGIS sub 52.1, p.12.***
21.	**Repetitive provision of assistance** Ambiguity as to whether requests can cover the repetitive provision of assistance, or are spent after the first performance of the specified conduct. Proportionality requirements and a maximum period of effect will be even more important if requests are intended to cover, and therefore confer immunity for, the repetitive provision of assistance. ***See: IGIS submission 1.1, p. 10.***	The Department indicates that s 21A(1) requests are intended to cover the repetitive provision of assistance. ***Home Affairs submission 16.1, Attachment B, p. 9.***	As per **comment no 11** above on TARs, TANs and TCN, IGIS suggests that s 21A(1) is amended to make explicit the intended application. This will facilitate both effective compliance and oversight. It will also promote clarity and consistency of decision-making about the making of requests (namely, by prompting the decision-maker to specifically consider whether the request should cover 'one-off' or 'ongoing' assistance, and specifically assessing the proportionality of that coverage). Further, IGIS considers that the stated intention for requests to cover the repetitive provision of assistance makes it more important that s 21A(1) is subject to specific proportionality requirements in the issuing conditions for requests, and that requests are subject to a maximum period of effect. ***See: IGIS submission 52, p. 56.***

Schedule 5—ASIO s 34AAA assistance orders (new coercive power)

[Note: blue rows denote key outstanding concerns identified in IGIS submission 1.1]

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
22.	**Not all assistance orders are required to specify essential matters** An assistance order is only required to specify certain essential matters (the compliance period, place of attendance and conditions on the order) if a computer has been removed from premises under a warrant. If a computer is accessed wholly remotely under a warrant, there is no requirement for orders to specify these matters, which may reduce transparency. ***See: IGIS submission 1.1, pp. 4, 11.***	The Department reiterates its previous evidence to the PJCIS, to the effect that the matters in s 34AAA(3) identified by IGIS as 'essential' are 'additional' requirements that are only necessary 'in these rare circumstances where assistance is required in relation to a computer or data storage device that is at a different location, not provided for by the issued warrant'. It is said that this 'provides the specified person with appropriate details given the change in location'. The Department also makes a number of observations about the entirely separate issue of issuing thresholds for computer access warrants. ***Home Affairs submission 16.1, Attachment B, p. 10.***	IGIS refers to our extensive submissions in response to the Department's previous evidence to the PJCIS review of the Bill. In short, IGIS considers that the matters identified by the Department as 'additional' safeguards are, in fact, essential in all orders, irrespective of whether a computer has been removed from warrant premises. This is particularly important in the case of computer access warrants under which data is accessed wholly remotely. A person who is subject to an assistance order would necessarily not attend the premises on which the target computer is located. It is also important because s 34AAA orders are capable of compelling assistance before a warrant is executed, and after a warrant is executed (including after it has expired). For example, a person may be required to attend ASIO-occupied premises to provide information that will help ASIO gain access to data under a warrant when that warrant is executed. A person may also be required to attend ASIO-occupied premises to provide assistance to ASIO in decrypting or otherwise making intelligible data that ASIO has already obtained under a computer access warrant (and did not remove a computer from warrant premises). Currently, the effect of s 34AAA(3) is that, in these circumstances, an assistance order ***would not be required*** to inform the person of the place at which they must attend, or the period of time during which they must render assistance, or any other conditions the Attorney-General has imposed on the order. IGIS maintains that this risks reducing transparency, to both the person who is subject to the order and to the Attorney-General in considering the terms of orders requested. It is also worth noting that ASIO's warrants have lengthy periods of effect (six months for computer access warrants) and can authorise access to multiple computers. ***[Continued]***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
			This increases the need for clarity and certainty on the face of ***all*** assistance orders. The Department's observations on the issuing thresholds for computer access warrants are not relevant to the ***separate issue*** of the conditions that must be included in an s 34AAA order. ***See: IGIS submission 52, pp. 61-62; IGIS submission 52.1, p. 9; IGIS submission 52.2 (in entirety).***
23.	**Arbitrary deprivation of liberty** There are no express safeguards against the risk that an order requiring a person to attend a place to provide assistance may result in an arbitrary deprivation of liberty. ***See: IGIS submission 1.1, pp. 4, 11.***	Home Affairs states that is 34AAA is not intended to result in the arbitrary deprivation of liberty, and that 'appropriate oversight and robust safeguards support these measures and ensure that requests are only issued where necessary'. ***Home Affairs submission 16.1, Attachment B, pp. 10-11.***	As noted in our previous submissions to the PJCIS on the review of the Bill, IGIS welcomes the statement of intention that s 34AAA is not intended to enable the arbitrary deprivation of liberty. However, the issue of concern to IGIS is that the provisions of s 34AAA do not appear to contain adequate safeguards to ensure that s 34AAA cannot be applied in a manner contrary to the stated policy intent. The matters identified as safeguards by the Department appear to place weight on the exercise of discretion by the Attorney-General in deciding whether issue an order and its terms, and the status of the Attorney-General as issuing authority. They do not address measures to ensure that the execution of an assistance order does not result in an arbitrary deprivation of liberty, or measures to ensure that the discretion to issue an assistance order could not be exercised in a manner that would result in an arbitrary deprivation of liberty. IGIS is particularly concerned that there is no requirement to ensure that a person attending premises in accordance with an assistance order is informed of their right to contact IGIS, and is given facilities to do so. IGIS is also concerned that there is no clear legal basis for IGIS to attend premises that a person is attending under an as 34AAA order (in contrast to IGIS's express powers in ss 9B and 19A of the *IGIS Act* in relation to ASIO's questioning and detention warrants). ***Continued***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
			The risk of arbitrary deprivation of liberty may also be increased by the absence of a requirement for all assistance orders to specify the place and duration of a person's attendance; and the absence of a statutory maximum duration for a person's attendance. IGIS also notes that there does not appear to be any information on the public record as to whether legal advice was obtained on the compliance of the scheme in s 34AAA with Australia's international human rights obligations. IGIS notes that the submission of the Australian Human Rights Commission on the Bill raised concerns about potential incompatibility with Article 9 of the *ICCPR* (the right to liberty and security of the person). ***See: IGIS sub 52, pp. 64-65; and IGIS sub 52.1,pp. 8-9.***
24.	**No obligation to cease action taken under an order where issuing grounds no longer exist** The Director-General of Security is not subject to a statutory requirement to take all reasonable steps to cease executing an assistance order, if he or she is satisfied that the issuing grounds have ceased to exist. (This is in contrast to a statutory obligation in relation to warrants under s 30.) ***See: IGIS submission 1.1, p. 4.***	The Department states that 'the existence of an assistance order is inherently linked to the timeframes for a warrant or ASIO operation' and that the Department and ASIO are 'open to addressing this issue through Ministerial Guidelines'. ***Home Affairs submission 16.1, Attachment B, pp. 11-12.***	IGIS welcomes the acknowledgement of the need for guidance on this matter. IGIS notes that there is a question of whether that form of guidance should be consistent with the statutory nature of guidance in relation to warrants currently in s 30 of the *ASIO Act*, so that both an assistance order and the underlying warrant are treated consistently. If the matter is to be managed via amendments to the ASIO Guidelines, IGIS is happy to be consulted in the development of those amendments. IGIS notes that guidelines may have the advantage of being able to be made more expeditiously than legislation, if there is a desire to do so. However, IGIS also notes that the recommendations of the PJCIS in 2014 and 2015 to review and update the Guidelines remain outstanding. (IGIS was last consulted on those amendments in June 2018.) ***See: IGIS submission 52, p. 63.***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
25.	**Persons who may be subject to an order** Assistance orders can be issued in relation to any person who is reasonably suspected of being involved in an activity that is prejudicial to security. This is not required to be an activity that is prejudicial to the security matter in respect of which the underlying warrant is issued, and could be any unrelated security matter. (IGIS is aware that the Department of Home Affairs gave evidence to the PJCIS that this broader application was not the intent.). ***See: IGIS sub 1.1, p. 11.***	The Department comments that 'it is critical that ASIO be able to compel assistance from persons suspected of involvement' and that 'there are many ways in which involvement may be made out'. It referred to examples of persons who are unintentionally acting as conduits for activities that are prejudicial to security, or persons who provide services to others who are engaged in prejudicial activities. ***Home Affairs submission 16.1, Attachment B, pp. 9-10.***	The Department's comments do not address the specific issue raised by IGIS, which is that s 34AAA(2)(c)(i) appears to enable an assistance order to be issued in relation to a person who is engaged, or suspected of being engaged, in ***completely unrelated prejudicial activities*** to the security matter specified in the relevant warrant. (That is, once a person is under suspicion of being engaged in ***any kind*** of prejudicial activities, this is sufficient to make them eligible to be the subject of an assistance order for any, or all, warrant operations being conducted by ASIO.) IGIS had queried whether this was intended, and a supplementary submission of the Department to the PJCIS review of the Bill appeared to suggest that this was not the intent. (Supplementary Submission 18.6 at p. 26 / QoN 70.) If there is an intention for s 34AAA(2)(c)(i) to be utilised in this way, then this intended usage will require an assessment of proportionality in the decision to seek an order and its terms. IGIS supports the inclusion of ***specific guidance*** in the *ASIO Guidelines* about the application of proportionality to the circumstances of requesting and executing s 34AAA orders. This would include guidance about proportionality in requesting and executing orders in relation to persons who are: (1) involved in prejudicial activities that are separate to the security matter specified in the warrant; or (2) in any case, unknowingly or unintentionally engaged in prejudicial activities, (eg, carriers or carriage service providers whose services may be used by other persons, such as customers, to undertake prejudicial activities). ***See: IGIS submission 52, pp. 60-61; IGIS submission 52.1, p. 8.***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
26.	**Retention / deletion of information obtained under an assistance order** No requirement for the DG 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 under the *ASIO Act*. (Such an obligation exists in section 31 in relation to information obtained under the underlying special powers warrant. Not all information obtained under an s 34AAA warrant will be covered by s 31 itself. (Eg, login credentials to a computer, including biometric identification information.) ***See: IGIS submission 1.1, p. 11.***	The Department comments that, 'as standard practice, ASIO appropriately protects information obtained in the course of their work. This could be addressed through Ministerial Guidelines'. ***Home Affairs submission 16.1, Attachment B, p. 11***	IGIS welcomes the acknowledgement of the need for additional parameters to be included in the ASIO Guidelines, and is happy to be consulted in the development of such Guidelines. IGIS notes, in particular, the need for the Guidelines to make specific provision for the handling of sensitive information obtained under s 34AAA assistance orders, such as login credentials or biometric identification information (and particularly parameters on access and secondary use). There is also a question as to what form any such parameters should take, and in particular whether they should be set in primary legislation (consistent with the requirement in relation to warrants in s 31) so that there is consistency between the parameters for information obtained under an s 34AAA order and information obtained under the relevant underlying warrant. ***See: IGIS submission 52, p. 63.***
27.	**Notification and service of orders** No statutory requirements for the notification and service of assistance orders on persons. ***See: IGIS submission 1.1, p. 11.***	The Department appears to suggest that there is no need for notice and service requirements on persons who are the subject of orders, due to the existence of annual reporting requirements and existing IGIS oversight functions. ***Home Affairs submission 16.1, Attachment B, p. 12.***	The Department's comments appear to misunderstand the concerns raised by IGIS about the absence of a notification and service requirement for s 34AAA orders. Given the coercive nature of s 34AAA orders, 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 additional availability of reporting requirements and IGIS oversight functions (particularly inspections) is valuable to the ***ex post facto review*** of ASIO's actions. This is complementary to, not a substitute for, a notification and service requirement. ***See: IGIS submission 52, p. 64; IGIS submission 52.1, p. 9.***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
28.	**Interaction with ASIO's questioning and detention warrants** No statutory guidance on the execution of an assistance order in relation to a person who is the subject of an ASIO questioning warrant or a questioning and detention warrant (including a role for IGIS, where in attendance for the compulsory questioning of a person). ***See: IGIS submission 1.1, p. 11.***	The Department states that, 'it is not sufficiently clear why it is considered necessary to prevent a section 34AAA order being made against the subject of an ASIO questioning warrant or questioning and detention warrant'. The Department also refers to IGIS's role in the oversight of questioning and questioning and detention warrants, and states that 'IGIS's general oversight function will allow them to audit both of these powers and any interaction between them'. It states that 'the Department does not consider separate statutory guidance necessary to provide IGIS further access to the use of these powers'. The Department also states it is working with IGIS in the development of a new legislative framework in response to recommendations of the PJIS review of ASIO's questioning and detention powers. ***Home Affairs submission 16.1, Attachment B, p. 12.***	The Department's comments appear to misunderstand both the substance of the concerns raised in IGIS's submissions on the Bill; and the nature of IGIS's statutory oversight functions in relation to ASIO questioning warrants (QWs) and questioning and detention warrants (QDWs). **Substance of IGIS's concerns** IGIS is not suggesting that QW or QDW subjects should be excluded from s 34AAA orders. Rather, IGIS is suggesting that there should be clear provision in the *ASIO Act* for how s 34AAA orders are to be executed against persons while they are in attendance under a QW, or are being detained under a QW or QDW. (For example, provisions dealing with the suspension of questioning to enable the execution of an s 34AAA order, including in relation to a computer (such as a smartphone) that is seized from the person under the QW provision in s 34ZB; and the status of a person who is being detained under a QW or QDW while they are in attendance under an s 34AAA order.) **Nature of IGIS oversight functions regarding QWs and QDWs** IGIS is given a specific oversight role for the execution of QWs and QDWs under Division 3 of Part III of the *ASIO Act*. This gives IGIS a function to be present at questioning. IGIS's powers to enter ASIO places of detention under the *IGIS Act* (for the purpose of inspections and inquiries) are limited specifically to places maintained under Division 3 of Part III of the *ASIO Act.* Consequently, these provisions do not provide a clear legal basis for IGIS to be present for the execution of an s 34AAA order against a person who is in attendance or being detained at a place under a QW or QDW. IGIS suggests that this uncertainty should be remedied expressly in the *ASIO Act*. **The need for clarification in current QW and QDW provisions** IGIS also notes that this issue arises in relation to the current QW and QDW provisions, and therefore its resolution cannot be deferred to the development and enactment of a new regime at some point in the future. ***[Continued]***

No.	IGIS suggestion *(in submission 1.1, summarised from previous submissions and evidence)*	Summary of Home Affairs comment *(from submission 16.1)*	IGIS further comments *(references are to IGIS submissions on the Bill)*
			In July and August 2018, IGIS had some preliminary engagement with the Department on a new QW regime, implementing recommendations of the PJCIS review of ASIO's questioning and detention powers. We have not had any engagement since this time, and have not seen any draft provisions. ***See: IGIS submission 52, p. 65.***

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone

Inspector-General of Intelligence and Security

12 October 2018

Contents

Summary

The Telecommunications and Other Legislation (Assistance and Access) Bill 2018 (the Bill) proposes to confer a range of significant new powers on intelligence and law enforcement agencies, to assist them in overcoming challenges presented by the use of encryption.

The Inspector-General of Intelligence and Security (IGIS) will oversee the exercise of the new powers by the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD). IGIS understands that the challenges faced by these agencies are significant, and makes no comment on the policy underlying the proposals in the Bill. The comments in this submission are limited to the oversight implications of the proposals.

This submission advances two main propositions. **First,** while the *Inspector-General of Intelligence and Security Act 1986* (*IGIS Act*) provides sufficient authority to oversee the new powers in relation to ASIO, ASD and ASIS, the proposed amendments would increase considerably the scope and complexity of oversight arrangements and the workload of this Office. The adequacy of resourcing to maintain effective oversight would require ongoing monitoring and reassessment.

Secondly, IGIS has identified a number of technical issues in various provisions that would present difficulties for independent oversight and would benefit from some targeted amendments. IGIS makes several suggestions to address apparent ambiguities and provide clear standards against which IGIS could conduct oversight of agency decision-making. Key issues are summarised below.

Key issues

1. **The absence of, or limitations in, reporting and notification requirements*:*** the lack of reporting or notification requirements about intelligence agencies' actions under the amendments in **Schedule 1** (in relation to ASIO, ASD and ASIS) and **Schedules 2 and 5** (in relation to ASIO) will make IGIS oversight difficult, particularly in relation to conferral and use of immunities from legal liability, and the exercise by ASIO of extended computer access-related powers. IGIS supports the inclusion of some further statutory reporting and notification requirements[1]

2. **A potentially unintended omission in authorised disclosure provisions**: the amendments to the *Telecommunications (Interception and Access) Act 1979* (*TIA Act*) in **Schedule 2** remove the existing lawful basis for the disclosure of certain interception information to, and by, IGIS officials for the purpose of performing oversight of ASIO. This appears to be unintended, and IGIS considers it important that there is no reduction in the existing authorisation.[2]

3. **The potential for intelligence agencies to make technical assistance requests for the voluntary creation of 'backdoors':** the amendments in **Schedule 1** do not limit the power of any agency to request communications providers to introduce, or omit to rectify, a systemic weakness or vulnerability into a form of electronic protection. It is unclear if this result is intended. If so, the task for IGIS in overseeing these requests will be complex, and would be assisted by a requirement for intelligence agencies to notify IGIS of any such requests when they are made.[3]

---

1 See the following parts of this submission: [1.4], [1.5], [1.6], [1.9] (Schedule 1); [2.1.3], [2.2.4], [2.2.7] (Schedule 2: ASIO warrants); [5.1.8] and [5.2.7] (Schedule 5: ASIO immunities and assistance orders).

2 See part [2.4] of this submission.

3 See part [1.3.4] of this submission.

4. **Powers of intelligence agencies to confer immunities from civil liability:** the amendments in **Schedules 1 and 5** will empower members of intelligence agencies to confer immunities from civil liability on various persons, with fewer safeguards than existing mechanisms by which such immunities are conferred.[4] IGIS would support closer alignment of safeguards to ensure consistency of decision-making about the conferral of immunities across different schemes; and to avoid the potential for propriety risks if there is a choice of immunities with differences in applicable thresholds, conditions and limitations.

5. **Powers of intelligence agencies to confer an effective immunity from criminal liability to certain computer offences:** the amendments in **Schedule 1** will also empower ASIO, ASIS and ASD to confer on communications providers an effective immunity from criminal liability to certain computer offences in the *Criminal Code*, in respect of conduct in accordance with a technical capability request, or a technical capability assistance notice in the case of ASIO. The scope of the effective immunity appears to be broader than immunities that would be available to members of ASIO, ASD and ASIS if they were to engage in the same conduct.[5] IGIS questions whether this is the intended result.

Other issues

Schedule 1—Industry assistance (new Part 15 of the *Telecommunications Act 1997*)

- Apparent ambiguities and inconsistencies in the various decision-making thresholds, conditions, limitations and procedural provisions governing the new industry assistance scheme.

- An anomaly in the disclosure offences applying to new Part 15, under which IGIS officials are require to discharge the evidential burden to an exception that they made the disclosure for the purpose of performing functions or duties as IGIS officials.

Schedule 2—Extensions of ASIO's warrant-based computer access powers

- Potential unintended consequences of the broad scope of the new telecommunications interception (TI) powers, and powers to temporarily remove computers and things from premises. Some of these consequences include:

    - the conferral of TI and temporary removal powers for the purpose of entering premises, and not only gaining access to relevant data held on, or accessible from, a computer; and

    - the conferral of a power to use force against persons and things to carry out TI.

Schedule 5—ASIO powers to confer civil immunities on persons providing assistance

- An absence of statutory requirements to ensure that the decision to confer a civil immunity on a person or body is reasonable and proportionate, and that the conduct of that person or body in reliance on the immunity remains reasonable and proportionate.

- The absence of a maximum period of effect for ASIO's requests for assistance, and consequently the civil immunity from liability that applies to persons who comply with such requests.

---

4 See the following parts of this submission: [1.1] and [1.4] (Schedule 1); and [5.1] (Schedule 5).

5 See part [1.5] of this submission.

- The absence of statutory limitations on the civil immunity in relation to conduct that causes significant pure economic loss, or physical or mental harm or injury, to a third party.
- Apparent gaps and ambiguities in procedural provisions, including oral requests and variations.

Schedule 5—Orders to assist ASIO in accessing data it has obtained under a warrant

- Ambiguities in, and the breadth of, the classes of persons whose assistance may be compelled.
- Limitations in safeguards to the issuing and execution of assistance orders, including:
    - the absence of a statutory requirement that ***all orders*** must prescribe important details, including the place a person must attend, and the period in which they must assist ASIO;
    - the absence of statutory safeguards against the exercise of multiple coercive powers in relation to a person who is the subject of a proposed assistance order;
    - the absence of specific requirements governing the collection, handling, secondary use and retention of sensitive information obtained under an order, such as biometric information;
    - the absence of clear safeguards against the risk that a person who is attending a place in accordance with an assistance order may be arbitrarily detained or deprived of liberty.

Background

The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018. The IGIS is an independent statutory officer who reviews the legality and propriety of the activities of the six agencies in the Australian Intelligence Community. Information about IGIS is at **Attachment A.**

Focus of this submission

If the Bill is passed, IGIS will oversee the exercise by ASIO, ASD and ASIS of the new powers conferred on them, several of which are significant extensions of existing powers. This submission explains how IGIS will conduct such oversight. Its content is reproduced substantially from the Inspector-General's unclassified submission to the Department of Home Affairs on the Exposure Draft Bill of 13 September 2018. IGIS does not make any comment on the policy underlying the Bill, but identifies a number of technical issues that would present difficulties for independent oversight, and could benefit from targeted amendments to the Bill. This submission covers:

- **Schedule 1 (industry assistance)**—new Part 15 of the *Telecommunications Act 1997*, to the extent that it will:
    - authorise ASIO, ASD and ASIS to confer immunity from civil liability on various communications providers who voluntarily render certain forms of technical assistance to those agencies in accordance with a ***technical assistance request*;**
    - empower ASIO to issue ***technical assistance notices*** to those providers to compel them to provide such assistance, with civil penalties for non-compliance; and
    - empower the Attorney-General to issue ***technical capability notices*** (on the request of ASIO) that compel communications providers to develop and maintain certain technical capabilities for the purpose of being able to provide technical assistance to ASIO (or to render technical assistance to ASIO) with civil penalties for non-compliance.
- **Schedule 2 (computer access)**—amendments to the *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*) to extend ASIO's warrant-based computer access powers to authorise the interception of telecommunications, the temporary removal of computers or other things from premises, and the concealment of activities done under a warrant after its expiry.
- **Schedule 5 (ASIO)**—amendments to the *ASIO Act* that will:
    - enable ASIO to confer immunity from civil liability on persons who voluntarily provide assistance to ASIO in the performance of its functions, in accordance with a request; and
    - empower the Attorney-General to make orders (on the request of ASIO) to compel persons to assist ASIO in accessing data held in, or accessible from, a computer or data storage device that is accessed or seized by ASIO under a warrant.

Resource impacts for IGIS

Oversight of the new powers will be complex and resource intensive. The adequacy of IGIS resourcing to maintain effective oversight (including complaint management and accessing independent technical expertise) will require ongoing monitoring, including as informed by the frequency and manner of use of the new powers by agencies.

Schedule 1—Industry assistance to ASIO, ASD and ASIS

Schedule 1 to the Bill proposes to insert a new Part 15 ('industry assistance') into the *Telecommunications Act 1997*. It would establish a scheme under which 'designated communications providers'[6] may be requested (under 'technical assistance requests')[7] or compelled (under 'technical assistance notices'[8] or 'technical capability notices'[9]) to provide various forms of assistance to security and law enforcement agencies, provided that the acts or things comprising the assistance are done in connection with the 'eligible activities'[10] of those providers.

If the Bill is passed, IGIS would oversee the actions of ASIO, ASD and ASIS in making and administering technical assistance requests, and the actions of ASIO in issuing and administering technical assistance notices.[11] IGIS would also oversee the actions of ASIO in making requests to the Attorney-General to issue technical capability notices, including oversight of the intelligence case accompanying the request, and any actions taken by ASIO in the administration of those notices.[12] This may include consideration of complaints from communications providers, and others who may be affected by the acts of communications providers pursuant to requests and notices.

1.1 Relationship with existing agency powers and immunities

A communications provider who engages in conduct in compliance with a request or notice will be immune from civil liability in relation to that conduct.[13] The Bill will also amend the *Criminal Code Act 1995* (*Code*) to protect providers from criminal liability in relation to the telecommunications service and computer offences in Parts 10.6 and 10.7 of the *Code* in these circumstances.[14]

1.1.1 Legal effect

As a general observation, the proposed amendments represent a significant change to the existing approach to the conferral of statutory immunities from legal liability on intelligence agencies and persons assisting those agencies in the performance of their functions. In particular:

- The existing arrangements relevant to ASIO are found in the special intelligence operations (SIO) scheme under Division 4 of Part III of the *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*). There are significantly more safeguards in the SIO scheme than those in new Part 15 of the *Telecommunications Act*. These include requirements for Ministerial-level approval;[15] proportionality and other requirements in the issuing criteria that limit the conduct able to be

6 New section 317C.

7 New Part 15, Division 2 (especially new section 317G).

8 New Part 15, Division 3 (especially new section 317L).

9 New Part 15, Division 4 (especially new section 317T).

10 New section 317C.

11 *Inspector-General of Intelligence and Security Act 1986* (*IGIS Act*), subsections 8(1)-(2) and section 9A.

12 *IGIS Act*, sections 8 and 9AA(b).

13 New paragraphs 317G(1)(c)-(d) (requests) and new section 317ZJ (notices).

14 Schedule 1, items 2 and 3 (new subsection 474.6(7A) and subparagraphs 476.2(b)(iv)-(vi) of the *Code*).

15 *ASIO Act,* sections 35B and 35C.

authorised;[16] exclusions of certain acts from the immunity;[17] and reporting and notification requirements to IGIS and the Attorney-General.[18]

- The current immunities from legal liability relevant to ASD and ASIS are in section 14 of the *Intelligence Services Act 2001* (*ISA*) and section 476.5 of the *Code.* They apply only to acts done by staff members and agents of those agencies outside of Australia, in the proper performance by those agencies of their functions,[19] and a limited set of preparatory actions (excluding acts for which ASIO would require a warrant or an authorisation to do in Australia).[20]

One effect of the amendments in Schedule 1 is that intelligence agencies will potentially have multiple grounds of statutory immunity from civil and criminal liability that they could apply to communications providers who perform functions for them, which apply different thresholds and are subject to different conditions and limitations.

It is conceivable that, in some circumstances, agencies will have a choice about which type or types of statutory immunity they will engage in a particular operation.[21] In some circumstances, agencies may engage multiple forms of immunity for various participants in an operation. They may potentially do so in conjunction with the exercise of authority under one or more warrants or other authorisations to undertake certain intrusive activities.

The task of performing oversight of agency operations that involve multiple sources of legal authority (including multiple sources of immunities, coercive collection powers and intrusive covert collection powers) will be complex, particularly where choices exist about the sources of relevant powers and immunities. Further, as the immunities conferred on communications providers under the scheme will remove third party rights to recover damages or obtain other legal remedies in relation to loss or damage caused by acts done pursuant to notices and requests, this may be a new source of complaints to IGIS.

1.1.2 General limits on technical assistance and capability notices (new section 317H)

New subsection 317ZH(1) provides that a technical assistance notice or a technical capability notice has no effect to the extent, if any, that it would require a designated communications provider to do an act or a thing that would require a warrant or an authorisation under any law of the Commonwealth or a State or Territory. Several Acts are identified specifically, including the *Telecommunications (Interception and Access) Act 1979* (*TIA Act*), *ASIO Act* and *ISA*.

---

16 *ASIO Act*, subsection 35C(2) especially paragraph (c).

17 *ASIO Act*, paragraph 35K(1)(e).

18 *ASIO Act*, sections 35PA and 35Q.

19 *ISA,* subsection 14(1); and *Code,* subsection 476.5(1).

20 *ISA,* subsections 14(2)-(2A); and *Code*, subsections 476.5(2)-(2A). (Note that the immunity for preparatory and ancillary conduct under the *ISA* is for acts done within and outside Australia, but in subsection 476.5 of the *Code* it is for acts done within Australia.

21 For example, **in the case of ASIO**, there may be a choice between the issuing of a technical assistance request and a request under new s 21A(1) of the *ASIO Act* (Schedule 5) or obtaining an authorisation for the provider as a participant in a special intelligence operation; or compelling assistance under a technical assistance notice or obtaining an order under new s 34AAA of the *ASIO Act* (Schedule 5). **In the case of ASIS and ASD** there may, in some circumstances, be a choice between the issuing of a technical capability request and engaging a provider as a consultant or contractor to provide services to the agency (thereby making them a 'staff member' of the agency under the *ISA* and enlivening the immunity in section 14 for certain acts done in the proper performance of the agency's functions).

New subsection 317ZH(2) further provides that it is to be assumed that each law imposing a warrant or authorisation requirement applies both within and outside Australia. This means that there would be neither any legal compulsion for a communications provider to render assistance to ASIO under a notice, nor any civil immunity for any such assistance rendered, if that assistance comprises, among other things:

- the interception of telecommunications, or accessing stored communications, metadata or telecommunications data from a carrier or carriage service provider (being activities for which ASIO would require a warrant or an authorisation under the *TIA Act*);[22]
- an activity for which ASIO would require a special powers warrant, a questioning warrant, an authorisation to collect foreign intelligence, or an authorisation to conduct a special intelligence operation under the *ASIO Act*;[23] and
- activities for which an *ISA* agency would require a Ministerial authorisation (including activities for the specific purpose of producing intelligence on an Australian person; certain activities by ASIS that will or are likely to have a direct effect on an Australian person; and activities by ASD for the specific purpose of preventing or disrupting cybercrime undertaken or enabled by an Australian person outside Australia).[24]

The intended effect of new section 317ZH appears to be that new Part 15 of the *Telecommunications Act* should not be used as a 'backdoor' method for agencies to collect intelligence or do related acts or things that would bypass their existing warrant or authorisation requirements.[25] This is an important safeguard. However, there are a number of uncertainties and potential gaps in the coverage of this provision (outlined below) which may make both compliance and oversight more complicated.

No limitations on technical assistance requests

New section 317ZH applies only to technical assistance notices and technical capability notices.[26] This raises the possibility that a technical assistance request could be given to a communications provider, asking it to voluntarily undertake collection activities for which the intelligence agency would require a warrant or an authorisation to carry out itself, in circumstances in which it would not be an offence for the communications provider to engage in that conduct. This may include circumstances in which a provider relies on an authorisation conferred by the amendments in item 3 of Schedule 1 to the Bill to avoid liability under the computer offences in Part 10.7 of the *Code*.[27]

---

22 New paragraph 317ZH(1)(a).

23 New paragraph 317ZH(1)(d).

24 New paragraph 317ZH(1)(e).

25 See also: Explanatory Memorandum, p. 68 at paragraph [265].

26 New subsection 317ZH(1).

27 For example, offences for the unauthorised impairment of electronic communication to or from a computer (*Code*, section 477.3); and unauthorised access to, or modification of, restricted data held in a computer (*Code*, section 478.1). The Explanatory Memorandum states, at p. 30, paragraph [16], that 'the powers in new Part 15 cannot authorise access, modification or impairment in circumstances where a warrant or authorisation would be required (new section 317SC of Part 15 makes this clear'. As Schedule 1 to the Bill does not contain a 'section 317SC', this may have been intended to be a reference to section 317ZH. As noted above, new section 317ZH only applies limitations to notices,

In such cases, the effect of the request would be that: the communications provider is immune from civil liability in relation to the activities; is immune from computer offences in relation to the causation of unauthorised access, modification or impairment of data held in or communications to or from a computer; and is entitled to payment by the agency in accordance with any contract made under new section 317K in connection with the request.

IGIS queries whether technical assistance requests are intended to be capable of use in circumstances in which they could effectively enable an agency to bypass statutory warrant or authorisation requirements. In any event, IGIS would consider that an intelligence agency would not be acting in the proper performance of its functions if it were to issue a technical assistance request to a provider to do an act or thing that the agency could not lawfully do without a warrant or an authorisation.

Suggestion: legislative clarification of the intended use of technical assistance requests

If there is no intention for technical assistance request to be used in these circumstances, as appears to be the case based on statements in the Explanatory Memorandum,[28] the limitation in new subsection 317ZH(1) could be amended to include requests, or an equivalent limitation could be expressly applied to the power of agencies to make requests under new section 317ZG.

The potential use of notices to compel a provider to do acts or things that are authorised under an extant ASIO warrant

Although new paragraphs 317ZH(4)(e) and (f) of the *Telecommunications Act* are expressed as being included merely 'to avoid doubt', these provisions appear to substantively qualify the limitation in new subsection 317ZH(1). They provide that the restrictions in new subsection 317ZH(1) do not prevent a notice from requiring a provider to give help to 'assist in, or facilitate, giving effect to a warrant', or to 'give effect to a warrant'.

The intended meaning of the words 'give effect' in this context is unclear. In particular, it is unclear if these words are intended to mean that notices could be used to compel communications providers to do the acts or things that are authorised under an ***extant*** special powers warrant or interception warrant that has been issued to ASIO and is in force during the compliance period for the notice.[29] It is similarly unclear whether the words 'give effect' are intended to cover warrants that are issued to ASIO after a notice is given but during the period of effect of the notice.

---

not requests, whereas the immunity in item 3 of Schedule 1 applies to conduct that is undertaken in accordance with a request. There does not appear to be any other provision in Schedule 1 to the Bill that would limit the power to make a technical assistance request to those circumstances in which the agency would not require a warrant or an authorisation to undertake the relevant act itself.

28 Explanatory Memorandum, p. 30 at paragraph [16].

29 The Explanatory Memorandum does not appear to provide meaningful insight into this issue. It states, at p. 69 at paragraph [268], that new subsection 317ZH(4) 'makes clear' that, notwithstanding subsections 317ZH(1) and (3), a notice can require a provider to assist in or facilitate giving effect to a warrant or an authorisation, or to give effect to a warrant or an authorisation.

Suggestion: legislative clarification of the intended meaning of the expression 'give effect'

As this type of ambiguity will make oversight more difficult, clarification of these matters would be desirable, preferably directly in the provisions of new section 317ZH.

Oversight implications for IGIS in relation to new s 317ZH(4)(f)

If the words 'give effect' in new paragraph 317ZH(4)(f) are intended to enable ASIO to issue notices that will compel communications providers to do acts or things that are authorised under an extant warrant, it would be necessary to determine the relationship between such a notice, and existing statutory requirements for the approval of persons to exercise authority under that warrant.[30]

In the absence of clear words to the contrary in new Part 15 of the *Telecommunications Act*, IGIS considers that the separate statutory authorisation requirements to exercise authority under a warrant would likely apply in relation to a communications provider, in addition to the issuing of the notice to compel them to do the relevant things.

The application of existing statutory authorisation requirements to exercise authority under one of ASIO's special powers warrants or interception warrants will be particularly important for oversight purposes if a ***single*** technical assistance notice issued to a provider is capable of compelling that provider to provide assistance to ASIO of a kind that could be used in ***multiple*** warrant operations that are carried out during the period of effect of the notice.

In these circumstances, the instrument authorising the provider to exercise authority under a particular warrant will be the primary record available to IGIS that links the compulsion of assistance under a notice with ***each*** warrant operation.

The relationship between 'listed acts or things' in new s 317E, actions requiring authorisation under ASIO special powers warrants, and the limitations in new s 317ZH

A technical assistance notice may require a provider to do one or more of the 'listed acts or things' specified in new section 317E.[31] However, several 'listed acts or things' appear to be acts or things for which ASIO would, or may depending on the facts, require a warrant or an authorisation to undertake itself.

This raises the question of how the limitation in new subsection 317ZH(1) and the qualifications in new paragraph 317ZH(4)(f) would apply to a notice that specified such 'listed acts and things'. For example, in some circumstances, ASIO may require a warrant to carry out the following 'listed acts or things' itself:

- The doing of acts or things under new paragraph 317E(1)(j) to 'conceal the fact that any thing has been done covertly in the performance of a function, or the exercise of a power, conferred by the law of the Commonwealth … so far as the function or power relates to … (iii) the interests of Australia's national security' would appear to cover activities carried out for the purpose of concealing acts or things done under one of ASIO's special powers warrants. However, those

30 See: *TIA Act,* section 12 (interception warrants) and *ASIO Act*, section 24 (special powers warrants).

31 New subsection 317L(3). (The type of assistance that can be required under a notice can include, but is not limited to, 'listed acts or things'.)

concealment-related actions generally require authorisation under the relevant special powers warrant, subject to the applicable statutory thresholds and conditions being met.[32]

- In some circumstances, it is possible that the doing of acts or things specified in new paragraphs 317E(1)(e)-(j) may cause a result that is prohibited or restricted under an ASIO special powers warrant. For example, ASIO's computer access warrants are subject to a limitation on the doing of acts or things that are likely to materially interfere with, interrupt or obstruct the lawful use of a computer, ***unless*** they are necessary to do one or more of the things specified in the warrant. These warrants also impose an absolute prohibition on the doing of acts or things that are likely to cause any other material loss or damage to lawful users of a computer.[33]

It appears to IGIS that new section 317ZH would operate to provide that a technical assistance notice would be legally effective in compelling a provider to give help in the circumstances outlined above ***only if:***

- ASIO was required to obtain, and had obtained, a special powers warrant authorising it to do the relevant acts or things;
- that warrant was in force for the period of effect (or compliance period, if any) of the technical assistance notice;
- the provider was authorised to exercise authority under that warrant in accordance with requirements under section 24 of the *ASIO Act*, and that authorisation was in force for the period of effect of the notice and the warrant; and
- the assistance purportedly compelled under the notice did not exceed the limits of the authority conferred under:
    - the warrant (including any statutory limitations on ASIO's warrant-based powers, or conditions imposed by the Attorney-General in respect of the particular warrant); or
    - the authorisation of the provider to exercise authority under the warrant.

Suggestion: statutory reporting requirements

Oversight of these matters is likely to be complex and would be significantly assisted by ASIO keeping written records that clearly link requirements in particular technical assistance notices to particular warrants and authorisation lists in relation to those warrants (being lists of the persons who are authorised to exercise authority under those warrants).

One way of facilitating consistent record keeping (and IGIS and Ministerial visibility) would be through amendments to the existing warrant reporting requirements in section 34 of the *ASIO Act* and section 17 of the *TIA Act.* These provisions could include a requirement to report if a person was compelled under a notice issued under Part 15 of the *Telecommunications Act* to do an act or a thing authorised under the warrant.

32 See, for example: *ASIO Act*, paragraphs 25(4)(e) (search warrants), 25A(c) (computer access warrants), 26BG(4)(g) and 26B(5)(i) (surveillance device warrants), 27A(1)(a) (FIC warrants) and the following authorities under identified person warrants: paragraphs 27D(2)(j) (search), 27E(2)(f) (computer access) and 27F(4)-(5) (surveillance devices). See further items 7, 8 and 12 in Schedule 2 to the Bill (new concealment powers in relation into computer access under ss 25A, 27A and 27E).

33 *ASIO Act*, subsection 25A(5), paragraph 27A(1)(a) and subsection 27E(5).

Relationship of the provision of 'technical information' under new paragraph 317E(1)(b) with ASIO questioning warrants, and the limitations in new subsection 317ZH(1)

A further ambiguity arises in relation to notices that compel the provision of 'technical information' under new paragraph 317E(1)(b) and the limitations in new section 317ZH.

Presently, for ASIO to compulsorily question a person to obtain information that is, or may be, relevant to intelligence that is important in relation to a terrorism offence, it must obtain a questioning warrant or a questioning and detention warrant under Division 3 of Part III of the *ASIO Act*.[34] However, it is conceivable that some 'technical information' sought to be obtained from a communications provider under new Part 15 of the *Telecommunications Act* may be relevant to intelligence that is important in relation to a terrorism offence.

It is unclear how the limitation in new paragraph 317ZH(1)(d) and the qualifications in new paragraphs 317ZH(4)(e) and (f) would apply, or are intended to apply, in these circumstances.

It is similarly unclear how new paragraphs 317ZH(1)(d) or (f) would apply in any other circumstances that are covered by another warrant or authorisation-based coercive power available to ASIO to collect intelligence, or information enabling the collection of intelligence. (For example, new section 34AAA of the *ASIO Act* in Schedule 5 to the Bill; or if ASIO's questioning warrant powers are in future expanded to enable questioning for the purpose of obtaining information that is important to the collection of intelligence relevant to all of the 'heads of security' under section 4 of the *ASIO Act*.)[35]

Similarly, the availability of new coercive powers, such as notices under new Part 15 of the *Telecommunications Act*, may have an effect on the issuing thresholds for other powers available to ASIO. For example, in order for ASIO to make a request for a questioning warrant, the Attorney-General must be satisfied that, having regard to other methods (if any) of collecting the intelligence that are likely to be as effective, it is reasonable in all the circumstances for the warrant to be issued.[36] In the absence of an explicit provision that removes overlap between the two schemes, the possibility of collection under a notice (or a request) under new Part 15 may need consideration as another collection method available to ASIO.

Suggestion: explanation of intended interaction of s 317ZH with ASIO questioning warrants

IGIS would be assisted by clarification of the intended application of the limitations in s 317ZH(1) in relation to assistance that involves a communication provider giving information to ASIO, in circumstances that are covered by the thresholds for issuing questioning warrants.

To avoid doubt, it may be desirable to consider the insertion of an express provision recording the intended interaction of new Part 15 of the Telecommunications Act with ASIO's questioning powers under Division 3 of Part III of the ASIO Act, in relation to technical assistance that consists of the provision of information.

---

34 *ASIO Act,* subsection 34D(4) and paragraph 34E(1)(b).

35 Such an extension was supported by ASIO and the Attorney-General's Department during the PJCIS inquiry into ASIO's questioning and detention powers. See: PJCIS, *Advisory Report on ASIO's Questioning and Detention Powers*, March 2018 at [3.13]-[3.32] and [3.125]-[3.128].

36 *ASIO Act,* paragraph 34D(4)(b).

Interaction of new Part 15 with the proposed amendments to the ASIO Act in Schedule 5

Similar interaction issues arise in relation to ASIO's use of the powers in new Part 15 of the *Telecommunications Act* in Schedule 1 to the Bill and the proposed amendments to the *ASIO Act* in Schedule 5 to the Bill. In particular, several provisions in each Schedule appear to cover the same ground, but are subject to different levels of authorisation, thresholds, conditions and limitations. These discrepancies are discussed in the comments below on Schedule 5.

Legal status of a provider who is rendering assistance to ASIO under a request or notice

In conducting oversight of ASIO's use of new Part 15 of the *Telecommunications Act*, IGIS will also need to consider the legal status of a communications provider who is rendering assistance under a request or a notice.

Depending on the circumstances, the provider might be taken to be an 'ASIO affiliate' within the meaning of that term in section 4 of the *ASIO Act*.[37] That status could provide a legal basis for the provider being subsequently authorised by ASIO to perform other functions or exercise other powers able to be conferred on ASIO affiliates, while the provider remains an ASIO affiliate. (However, while it seems likely that a provider who is subject to a request would be an ASIO affiliate, there may be some ambiguity as to whether a provider who is ***compelled under a notice*** to provide assistance to ASIO could fall within the definition of an 'ASIO affiliate'.)[38]

Separately to the potential status of a provider as an 'ASIO affiliate', there is also some ambiguity as to whether a provider could be taken to be an 'entrusted person' for the purpose of the general secrecy offences under Division 1 of Part III of the *ASIO Act* for unauthorised communication of, or dealing with, certain information.[39] If so, providers could be subject to disclosure offences under the *ASIO Act,* in addition to the disclosure offences in new section 317ZF of the *Telecommunications Act* (and potentially general secrecy offences, such as those in Division 122 of the *Criminal Code*). The disclosure offence in subsection 18(2) of the *ASIO Act* for the unauthorised communication of

37 An 'ASIO affiliate' means a person performing functions or services for ASIO in accordance with a contract, agreement or other arrangement.

38 In particular, there appears to be some doubt that a notice could be a form of 'other arrangement' for the purpose of the definition of an 'ASIO affiliate' in section 4 of the *ASIO Act*. There is an argument that the words 'other arrangement' are limited by the preceding words 'contract' and 'agreement' so as to require some kind of ***voluntary relationship*** with ASIO under which a person agrees, without being subject to any legal compulsion, to perform functions or services for ASIO. For this reason, it is also arguable that the words 'contract' and 'agreement' in the definition of 'ASIO affiliate' should be read down to exclude 'agreements' between ASIO and a communications provider about the terms and conditions on which the provider will comply with requirements set out in a technical assistance or capability notice (as contemplated in new paragraph 317ZK(4)(a) of the *Telecommunications Act*).

39 See the definition of an 'entrusted person' in section 4 of the *ASIO Act*, which is an ASIO employee, an ASIO affiliate or 'a person who has entered into a contract, agreement or arrangement with ASIO (other than as an ASIO affiliate)'. (See also the unauthorised communication offence in subsection 18(2) of the *ASIO Act,* which does not use the term 'entrusted person' but its elements in paragraph 18(2)(b) cover the substance of the definition of that term.) It is arguable that the words 'entered into' and 'arrangement' denote the ***voluntary*** entry into a relationship with ASIO, and therefore exclude a relationship that is brought into existence by the exercise of a coercive power.

information is punishable by a maximum penalty of 10 years' imprisonment, in contrast to the five-year maximum penalty in new section 317ZF of the *Telecommunications Act*.[40]

Further, a provider who acts in accordance with a technical assistance request or a notice issued by ASIO that amounts to the exercise of authority under one of ASIO's warrants (assuming that this is permissible under new section 317ZH) may also be taken to be a 'member' of ASIO for the purpose of subsection 3(1) of the *IGIS Act*. (That is, a person who is authorised to perform the functions of ASIO, for and on its behalf.) In this event, the legality and propriety of the provider's actions would be ***directly*** subject to IGIS oversight, ***as the actions of ASIO***, under sections 8, 9 and 9A of the *IGIS Act*.[41]

Suggestion: reporting and notification requirements

This would have resource implications for IGIS, and would also require ASIO to provide early notification to IGIS of the making of requests or issuing of notices (see further **[1.9] below** in relation to reporting).

Similar issues would arise in relation to the status under the *IGIS Act* of communications providers who render assistance to ASIS and ASD in accordance with a request. It would be reasonable for a provider to be informed of these matters by the relevant Director-General or delegate when a request or notice is given.

Ambiguities in the application of the Ministerial authorisation-related limitation in new paragraph 317ZH(1)(e)

New paragraph 317ZH(1)(e) provides that technical assistance and capability notices are of no effect if they require a provider to do an act or thing for which a Ministerial authorisation is required under the *ISA*. There are several potential ambiguities and complexities in the application of this safeguard (explained below). These issues arise because the agencies that are subject to the Ministerial authorisation requirements in the *ISA* have no ability to issue technical assistance notices, or to request technical capability notices.

Suggestion: clarification of intended application of s 317ZH(1)(e) to ASIO and 'interception agencies 'issuing technical assistance notices, or requesting technical capability notices

IGIS supports clarification of the intended application of new paragraph 317ZH(1)(e) in relation to ASIO and the 'interception agencies' which may issue technical assistance notices or request the Attorney-General to issue technical capability notices under new Part 15.

40 The same issue also applies in relation to the status of designated communications providers who render voluntary assistance to ASIS or ASD in accordance with a technical assistance request. Sections 39 and 40 of the *ISA* contain offences for the unauthorised communication of information that relates to the functions of ASIS or ASD by persons who are in a 'contract, agreement or arrangement' with ASIS or ASD. These offences are punishable by a maximum penalty of 10 years' imprisonment, in contrast with the maximum penalty of five years applying to new s 317ZF.

41 See: *IGIS Act*, subsection 3(3), which deems the action taken by a member of a 'Commonwealth agency' (which includes ASIO and the ISA agencies) to be that of the agency if the member takes the action in his or her capacity as a member.

Uncertainty about the relevance of Ministerial authorisation requirements in the ISA

It is unclear if a limitation based on the Ministerial authorisation requirements in the *ISA* would have any effect. The *ISA* Ministerial authorisations requirements do not apply to ASIO or 'interception agencies' within the meaning of new Part 15 of the *Telecommunications Act*.[42] Further, the functions and powers conferred on *ISA* agencies (namely, ASD and ASIS) under new Part 15 of the *Telecommunications Act* are limited to technical assistance requests, and new section 317ZH does not apply to those requests (only to technical assistance and capability notices, which are available to ASIO). Further, the issuing criteria for technical assistance and capability notices appear to limit the assistance able to be compelled under a notice to acts and things that are linked to the functions of the issuing or requesting agency (ASIO and 'interception agencies) whereas the Ministerial authorisation requirements in the *ISA* are linked to the functions of the *ISA* agencies.[43]

As a general principle of statutory interpretation, all words in a provision must be given some meaning and effect, as the Parliament is presumed not to have enacted a provision that has no practical effect.[44] An alternative reading is that new paragraph 317ZH(1)(e) applies the *ISA* Ministerial authorisation requirements as limitations on the requirements that may be specified in technical assistance and capability notices, notwithstanding that these notices may only be issued or sought by agencies ***other than*** the *ISA* agencies. In particular, this interpretation would mean that:

- if ASIO or an 'interception agency' was to issue a notice (or if the Attorney-General was to issue a capability notice on the request of ASIO or an 'interception agency'), then
- that notice could not compel a provider to do an act or thing for which ***ASIS or ASD*** would require a Ministerial authorisation, if ASIS or ASD were to do the act or thing specified in the notice for the purpose of performing ***their*** respective functions.

Broader interpretive implications for new section 317ZH

If the intended interpretation is as outlined above, then the same reasoning would presumably apply in relation to ***all*** of the laws listed in new paragraphs 317ZH(1)(a)-(g). For example, if the issuing or requesting agency in relation to a notice was ASIO, then new section 317ZH would provide that the notice has no effect if the AFP would require a warrant or an authorisation under the *Crimes Act* or *Surveillance Devices Act* to undertake the activity, even if it would not be necessary for ASIO to obtain a warrant or an authorisation under its governing legislation.[45]

If this is the intended interpretation, then the application of new section 317ZH is likely to be extremely complex to administer and oversee, because it would require a review of the application of ***all of the specific Acts*** listed in new paragraphs 317ZH(1)(a)-(e) in relation to ***any or all*** of the entities which are governed by the warrant or authorisation-based powers conferred under those Acts. New paragraphs 317ZH(1)(f) and (g) would further require a review of ***any and all other*** Commonwealth, State and Territory laws that would require ***any entity*** governed by them to obtain

42 New subsections 317L(1) and 317T(1).

43 New paragraphs 317L(2)(a)-(c) and new subsections 317T(2) and (3).

44 *Commonwealth v Baume* (1905) 2 CLR 405 at 414 (per Griffith CJ).

45 This could arise where there is an offence-specific exception in favour of ASIO (or classes of persons that cover ASIO employees and ASIO affiliates) that does not also cover AFP members, or where the elements of an offence do not cover ASIO personnel, but could or do cover AFP personnel.

a warrant or an authorisation to undertake an activity of the kind that is specified in the technical assistance or capability notice.

A similar point can also be made in relation to new subsection 317ZH(3), which would require an assessment of whether any proposed use of a surveillance device or access to data held in a computer by a provider would require a warrant under State or Territory surveillance laws. This would be particularly complex in view of differences in individual State and Territory provisions (including relevant definitions and application provisions).

Specific interpretive implications for new paragraph 317ZH(1)(e)

If the intended interpretation is as outline above, then some further difficulties arise in relation to new paragraph 317ZH(1)(e). In particular:

- Some Ministerial authorisation requirements in the *ISA* are tied to matters that are specified in Ministerial directions.[46] This means that the substance of any limitation applied by new paragraph 317ZH(1)(e) of the *Telecommunications Act* may vary depending on the particular Ministerial directions under the *ISA* that are in force from-time-to-time.
- In some circumstances, ASIS does not need a Ministerial authorisation if it undertakes certain activities outside Australia involving the production of intelligence on an Australian person for the purpose of assisting ASIO, generally at the request of ASIO.[47] This means that the application of the limitation in proposed paragraph 317ZH(1)(e) of the *Telecommunications Act* may depend on the precise purpose for which the communications provider was required to give assistance.

These matters would make IGIS oversight complex, and would likely make it impossible for a communications provider to make a meaningful assessment of its legal position under new paragraph 317ZH(1)(e). Unlike IGIS, a communications provider is unlikely to have access to the necessary information, as the relevant Ministerial directions given under the *ISA* are not legislative instruments and are normally classified.[48]

46 *ISA,* paragraphs 8(1)(a)(ii) (in relation to certain activities of ASIS); and 8(1)(b).

47 *ISA,* Part 2, Division 3 (ASIS assistance to ASIO).

48 *ISA,* subsections 6(3A) and 8(5). This is also the position in relation to requests made of ASIS by ASIO for the purpose of Division 3 of Part 2 of the *ISA*: subsection 13B(8).

1.2 Decision-making criteria for requests and notices

1.2.1 Assessment of proportionality

Technical assistance requests (new s 317G)

There is no statutory requirement for the Directors-General ASIO, ASD or ASIS (or their delegates)[49] to consider, and be satisfied of, the proportionality or reasonableness of any immunity from civil liability as a pre-condition to making a request under new section 317G. For example, there is no requirement for the Directors-General or their delegates to consider:

- the importance of the particular assistance sought to the performance by the agency of its functions; and
- whether it is reasonably foreseeable that the conferral of immunity may have an adverse impact on innocent third parties who may suffer loss or damage, and would be deprived of a right to a legal remedy against the person, and if so, whether:
    - the national interest in performing the relevant function for which the assistance is sought is proportionate to the effect of the immunity on the rights of innocent third parties;
    - the assistance sought could be provided in a way that avoids or minimises the risk of causing loss or damage to an innocent third party; and
    - any alternatives are available to the conferral of a complete immunity from civil liability. (For example, the provision of an indemnity to the provider whose assistance is requested, via the making of an ordinary agreement rather than engaging new section 317G.)

The Explanatory Memorandum appears to suggest that the routine consideration of matters of proportionality could be inferred from the seniority of the relevant decision-maker (the Director-General or delegate who must be at least an acting SES Band 1 or a 'coordinator').[50] In the experience of IGIS, a statement of expectation or subjective policy intent about the way in which a discretionary decision-making power should be exercised has considerably less force in promoting sound and consistent decision-making than an explicit statutory requirement.

The value of a statutory decision-making condition

A statutory requirement for a decision-maker to assess specified matters as a pre-condition to making the relevant decision ensures that the relevant matters are clearly drawn to the attention of the decision-maker in each case. Further, in the experience of IGIS, a statutory requirement is the most effective way of facilitating better practice by agencies in keeping appropriately detailed and consistent record-keeping about their decisions to exercise a discretionary power. This ensures that the relevant decision-making process is auditable, including by IGIS.

In the absence of a statutory requirement to consider the proportionality and reasonableness of the conferral of a civil immunity on a communications provider through the making of a request under

49 See the powers of delegation in new sections 317ZN, 317ZP and 317ZQ. They allow the Directors-General of ASIO, ASIS and ASD to delegate their functions and powers under new Part 15 to, respectively, ASIO affiliates and ASIO employees, and staff members of ASIS and ASD, who hold SES positions, or the position of 'coordinator' in the case of ASIO.

50 Explanatory Memorandum p. 43 at paragraph [88].

new section 317G, IGIS would assess matters of proportionality and reasonableness in considering the propriety of agencies' decision-making about the making of a request. IGIS expects that agencies will develop internal policies and guidelines on the exercise of powers under new section 317G, which include proportionality considerations in relation to the conferral of civil immunity. Further, IGIS would regard the general requirement in paragraph 10.4(a) of the current *Ministerial Guidelines to ASIO* (issued under section 8A of the *ASIO Act*) as relevant to ASIO's decisions to confer civil immunity under new section 317G. Paragraph 10.4(a) provides that any means used for obtaining information must be proportionate to the gravity of the security threat posed and the probability of its occurrence.

Suggestion: statutory decision-making criteria **and** administrative guidance on proportionality

The insertion of express statutory proportionality requirements in new section 317G, similar to those in new sections 317P and 317RA for technical assistance notices,[51] would provide clear and consistent standards against which IGIS could conduct oversight of intelligence agencies' decision-making.

There would also be value in updating existing administrative guidance on the assessment of proportionality in applicable Ministerial guidelines, including the guidelines issued to ASIO under section 8A of the *ASIO Act,* to deal specifically with the exercise of powers to make requests (and thereby enliven immunities).

Technical assistance and capability notices (new ss 317P, 317RA, 317V and 317ZAA)

New sections 317P and 317RA contains some decision-making criteria that would require the Director-General of Security (or delegate) to take into account various considerations about the proportionality, reasonableness, practicality and feasibility of the requirements proposed to be specified in a technical assistance notice.

This includes a requirement in new paragraph 317P(a) for the Director-General or delegate to be satisfied that the requirements imposed by the notice are reasonable and proportionate. Equivalent requirements apply to variation decisions under new section 317Q.[52]

The assessment of reasonableness and proportionality

New section 317RA provides that the Director-General or delegate must, in considering whether the requirements in a technical assistance notice, or a varied notice, are reasonable and proportionate, have regard to a number of specified matters. These include the interests of national security and law enforcement; the legitimate interests of the communications provider; the objectives of the notice; the availability of other means to achieve the objectives; the legitimate expectations of the Australian community relating to privacy and cybersecurity; and such other matters as the Director-General considers relevant as the case requires.

---

51 New section 317P requires the Director-General of Security to be satisfied that the requirements imposed by the notice are 'reasonable and proportionate' and that compliance is 'practicable and technically feasible'. New section 317RA prescribes a number of matters that must be taken into consideration. (But note the comments below, suggesting that more detailed decision-making criteria could usefully be included in new section 317RA for the purpose of new section 317P.)

52 New subsection 317Q(10).

IGIS welcomes the inclusion of these requirements, which will assist in promoting consistency of decision-making and record-keeping, and will provide clear and transparent benchmarks against which IGIS will conduct oversight of issuing and variation decisions.

However, IGIS notes that there is no specific requirement for the Director-General to consider the potential impact on third parties who may be adversely affected by the conferral of civil immunity due to the loss of a right to a legal remedy for any loss, damage or injury caused by the providers actions in compliance or purported compliance with a notice. IGIS concurs with the statement in the Explanatory Memorandum that the concepts of reasonableness and propriety would require consideration of this matter in each case.[53]

Suggestion: an additional statutory consideration—impact of immunity on third parties

IGIS considers that there would be benefit in adding this to the list of mandatory considerations to ensure consistency of consideration and record-keeping.

Consideration might also be given to updating the *Minister's Guidelines to ASIO*, issued under section 8A of the *ASIO Act*, to provide further and more detailed guidance on the assessment of the reasonableness, proportionality and technical feasibility of proposed requirements in technical assistance notices.

Equivalent decision-making criteria to those in new sections 317P, 317Q and 317RA apply to the Attorney-General in relation to the issuing and variation of technical capability notices under new sections 317V, 317X and 317ZAA,. While IGIS would not review the decisions of the Attorney-General, the advice provided by ASIO as part of a request for the issuing or variation of a notice would be subject to IGIS oversight.

Accordingly, statutory or administrative guidance (or both) about the consideration of impacts of a civil immunity on innocent third parties could also aid oversight of IGIS oversight of ASIO's requests to the Attorney-General for the issuing or variation of a capability notice, including its advice on the proportionality-related requirements in new sections 317V and 317Z.

Exercise of multiple coercive powers in relation to a communications provider

The decision-making criteria for issuing technical assistance and capability notices do not specifically require the decision-maker to take into account the potential for oppression as a result of the exercise of multiple coercive powers against an individual communications provider, in relation to the same or substantially similar subject matter.[54] (This includes either a stand-alone requirement; or specifically in the matters that must be taken into consideration under new sections 317RA and 317ZAA in assessing the reasonableness and proportionality of a notice.

In particular, the general requirement in new paragraphs 317RA(c) and 317ZAA(c) to consider the 'legitimate interests' of the provider does not necessarily provide a clear directive to routinely consider the cumulative impact of the exercise of multiple coercive powers against them.)

53 Explanatory Memorandum, p. 49 at paragraph [132].

54 Compare the requirements for requests for questioning and detention warrants in *ASIO Act*, paragraphs 34D(3)(c)-(d) and 34F(3)(c) and (d). These requests ***must*** include information about previous requests or warrants issued in relation to the person. These matters are then able to be taken into consideration by the Attorney-General in deciding whether to approve the request.

The risk of oppression to a provider may arise in multiple scenarios in which a notice has been issued, or is proposed to be issued, including:

- the issuing by ASIO of multiple technical assistance notices to a particular provider, or the issuing by the Attorney-General of multiple capability notices in relation to a particular provider on the request of ASIO;
- the issuing of multiple technical assistance or capability notices to a particular provider by, or at the request of, several different agencies under new Part 15;
- the exercise by ASIO of coercive powers against a particular provider under multiple laws (such as, technical assistance notices, questioning warrants, and orders to provide technical information or assistance under new section 34AAA of the *ASIO Act* in Schedule 2); and
- the exercise of different types of questioning and other coercive information-gathering powers against a provider by multiple agencies under their respective governing legislation (for example, certain police powers, ACIC examinations and the ASIO powers noted above).

Suggestion: statutory requirement to consider the exercise of multiple coercive powers

IGIS considers that amendments to the statutory requirements of reasonableness and proportionality in decision-making about the issuing of notices in new sections 317P, 317RA, 317V and 317ZAA could provide an effective means of managing this risk, and for IGIS to conduct oversight of this aspect of agencies' decision-making in issuing or requesting notices (as applicable).

These provisions could include:

- in the case of decisions to issue technical assistance notices, a requirement for the decision-maker to assess the potential for oppression arising from the exercise of multiple coercive powers against a provider in line with the above; and
- in the case of requests for technical capability notices, a requirement for the requesting agency to provide information to the Attorney-General about any previous requests made and notices issued, and information about the exercise or proposed exercise of other coercive powers in relation to the provider.

These requirements would also need to be supported by arrangements between agencies for the sharing of relevant information about the exercise or proposed exercise of coercive powers.

1.2.3 Linkage of assistance to agency functions (new ss 317G(2), 317L(2) and 317T(2))

Requests and notices are linked to the giving of help in relation to the performance of functions or exercise of powers by agencies that relate to specified matters. These include the following:

- ***In the case of technical assistance requests***—agency functions or powers that are linked to criminal law enforcement and the enforcement of pecuniary penalty provisions, or protecting the interests of Australia's national security, foreign relations or national economic well-being.[55]
- ***In the case of technical assistance and technical capability notices***—agency functions or powers that are linked to criminal law enforcement and the enforcement of pecuniary penalty provisions, or safeguarding national security (but not the interests of Australia's foreign relations or national economic well-being).[56]

Technical assistance requests—linkage to functions of ASD and ASIS

In the case of technical assistance requests made by ASD and ASIS, references in new section 317G to functions or powers relating to Australia's interests in national security, foreign relations and national economic well-being have a clear link to the functions and powers of ASIS and ASD, as subsection 11(1) of the *ISA* uses these expressions in delimiting those agencies' functions.

Technical assistance requests and notices—linkage to functions of ASIO

In the case of technical assistance requests and notices issued by ASIO, and technical capability notices requested by ASIO, the expressions 'the interests of Australia's national security' (new section 317G) and 'safeguarding national security' (new sections 317L and 317T) are not identical to the defined term 'security' in section 4 of the *ASIO Act,* which is central to ASIO's functions in section 17 of that Act. This will potentially make it complex to identify links to ASIO's functions and powers in some cases. However, as the ordinary meaning of the term 'national security' appears to be narrower than the meaning of the defined term 'security' in the *ASIO Act*,[57] new sections 317G, 317L and 317G may serve a limiting function in respect of the matters that may be the subject of a request or notice made or requested by ASIO.

Potential ambiguity—law enforcement-related functions

The references in new sections 317G, 317L and 317T to agency functions that relate to criminal law enforcement and the enforcement of pecuniary penalties[58] are not directly relevant to the functions of ASIO, ASD or ASIS, given that these agencies' governing statutes expressly provide that their functions do not include the enforcement of the law.[59]

---

55 New paragraph 317G(2)(b) and new subsection 317G(5).

56 New paragraph 317L(2)(c) and new subsections 317T(2) and 317T(3).

57 In particular, the concept of 'national security' may not cover the matter in paragraph (b) of the definition of 'security' in section 4 of the *ASIO Act,* being 'the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa)'.

58 New paragraphs 317G(5)(a)-(c), 317L(2)(c)(i)-(iii) and 317T(3)(a)-(c).

59 *ISA,* subsection 11(2) and *ASIO Act*, subsection 17(2).

Suggestion: legislative clarification of application in relation to ASIO, ASD and ASIS

It is unclear whether these provisions of new sections 317G, 317L and 317T are intended to have some indirect application to ASIO, ASD and ASIS. (For example, by reason of the exceptions to the prohibition on law enforcement functions in paragraphs 11(2)(c), (d) and (f) and subsection 11(3) of the *ISA,* or the cooperation functions of ASIO in paragraph 19A(1)(d) of the *ASIO Act*.)[60]

IGIS would support clarification of the intended application, preferably in the provisions of new sections 317G, 317L and 317T.

Differences between new Part 15 and obligations to give help in existing section 313

IGIS acknowledges that the obligations imposed on telecommunications carriers, carriage service providers and intermediaries in existing subsections 313(3) and 313(4) of the *Telecommunications Act* use a broadly similar drafting formula to the proposed references to agency functions in new sections 317G, 317L and 317T.[61]

However, IGIS notes that the powers to compel specific forms of assistance in notices issued under new Part 15 are of a materially different character to the general obligation to provide 'such help as is reasonably necessary' in existing subsections 313(3) and 313(4). The coercive powers in new Part 15 also apply to a considerably larger range of entities than telecommunications carriers, carriage service providers and intermediaries.

Further, new Part 15 proposes to confer immunities from civil liability on communications providers, whereas existing section 313 confers only an immunity to an action or other proceeding ***for damages*** (and not from other ***non-pecuniary remedies*** such as injunctions or specific performance, which may be of considerable value to innocent third parties who would be prevented by new Part 15 from seeking such orders to restrain a communications provider from causing further loss or damage as a result of compliance with a request or notice).[62]

IGIS suggests that these significant differences between existing sections 313(3) and 313(4) and new Part 15 of the *Telecommunications Act* give rise to a greater need for legal certainty in the

60 The Explanatory Memorandum states, at p. 44 at paragraph [96], that the provision is intended to cover 'precursory and secondary intelligence gathering activities that support the investigation and prosecution of suspected offences'. However, it is not entirely clear how, if at all, this statement is intended to apply to the exceptions in subsections 11(2) and 11(3) of the *ISA* in the context of the 'relevant objectives' of technical assistance requests made by ASIS and ASD.

61 Subsections 313(3) and (4) of the *Telecommunications Act* provide that carriers, carriage service providers and carriage service intermediaries must, in connection with the operation of telecommunications networks or facilities or the supply of services, provide such help as is reasonably necessary to officers of any Commonwealth, State or Territory authority for specified purposes. These purposes cover criminal law enforcement and laws imposing pecuniary penalties, protection of the public revenue, and safeguarding national security. These purposes **do not include** matters concerning foreign relations or national economic well-being. (Cf: Explanatory Memorandum, p. 44, paragraph [92] which states that the agency functions referred to in new subsection 317G(5), including in relation to Australia's interests in foreign relations and national economic well-being, are '***consistent with*** the purposes for which agencies currently seek assistance from domestic carriers and carriage service providers under section 313 of the *Telecommunications Act*.)

62 *Telecommunications Act,* subsection 313(5).

application of new Part 15, and therefore merit a greater degree of precision in the drafting of new sections 317G, 317L and 317L, in relation to their application to the functions of particular agencies.

The fact that the powers in new Part 15 will be available to a far more constrained group of agencies than 'authorities of the Commonwealth and of the States and Territories' (as is the case for the obligations in existing section 313) also suggests that more precise drafting is feasible in relation to new Part 15 than may be feasible for the scheme in existing subsections 313(3) and 313(4).

1.3 Conditions of assistance to be provided under a request or notice

1.3.1 Absence of a fixed maximum period of effect (new ss 317HA, 317MA and 317TA)

Technical assistance requests issued by the Directors-General of ASIO, ASD and ASIS and notices issued by the Director-General of Security (or their delegates) are subject to a 'default' period of effect of 90 days from when the notice or request was given.[63] Technical capability notices are subject to a 'default' period of effect of 180 days from issue.[64]

However, these 'default' periods only apply if the request or notice does not specify an expiry date. If a request or a notice specifies an expiry date, then it is taken to be in force until the start of the expiry date (unless revoked sooner).[65] It therefore appears to be possible for a decision-maker to prescribe an expiry date which is ***longer than*** the 'default' period with no fixed upper limit on the prescribed period of effect.

IGIS notes that, from the perspective of both legality and propriety, there are many advantages in prescribing a fixed maximum period of effect for a coercive or intrusive power. The power to compel the provision of assistance, and the power to extinguish third parties' rights to remedies by the conferral of an immunity from civil liability meet this description.

The value of a fixed maximum period of effect

The imposition of a fixed maximum duration creates a trigger for a new issuing decision. This effectively requires a periodic re-assessment of the grounds for issuing requests and notices and their specific terms (including consideration of any changes in circumstances).

Even if there is no statutory limit on the number of requests or notices that could be issued subsequently, these periodic reviews would aid oversight and accountability, and would be consistent with most other intelligence warrants and other powers, which have a fixed maximum period of operation, subject to renewal. The discretion conferred on the issuing authority in relation to the period of effect is normally to impose a ***shorter period*** than the statutory maximum, not a ***longer period***, as appears to be permitted under new paragraphs 317HA(1)(b)(i), 317MA(1)(b)(i) and 317TA(1)(b)(i).

63 New sections 317HA and 317MA.

64 New section 317TA.

65 See paragraph (1)(b) of each of new sections 317HA, 317MA and 317TA.

Suggestion: a statutory maximum period of effect

IGIS would support a limitation on the power of the decision-maker to set an expiry date, specifically through the insertion of a statutory maximum period of effect that is aligned with the 'default' period of effect if no expiry date is specified (being 90 days or 180 days).

Further suggestion: qualification of powers of variation in relation to extensions

Further, since there are explicit powers to vary requests and notices in new sections 317JA, 317Q and 317T, IGIS considers that there would be benefit in including a provision to make explicit that a variation which extends (or further extends) the period of effect of a request or notice cannot extend the total period beyond the applicable statutory maximum. This would be consistent with existing provisions of the *ASIO Act* that limit powers of variation in relation to the duration of special powers warrants and authorities for the conduct of special intelligence operations.[66]

1.3.2 Revocation requirements in relation to notices

Technical assistance and capability notices are also subject to revocation requirements. These provisions impose an obligation on the relevant decision-maker to revoke the notice, if he or she is satisfied that the requirements are not reasonable or proportionate, or if compliance is not practicable or technically feasible.[67]

There is no positive obligation on the decision-maker to consider ***whether*** the grounds for mandatory revocation are met during the period in which the notice is in force. Nor is there any positive obligation on the decision-maker to consider any representations that are made by the provider about the revocation of a notice. Nor are there obligations on agency staff members to bring information to the attention of the decision-maker that suggests that the grounds of issuing have ceased to exist.[68] In practice, this may limit the effectiveness of the revocation requirements.

The absence of such obligations may be particularly problematic in the absence of a fixed maximum period of effect for those notices that specify an expiry date under new subparagraphs 317MA(1)(b)(i) and 317TA(1)(b)(i). (Noting that the absence of a statutory maximum period creates the potential for notices to remain in force for prolonged periods of time, which could be far in excess of the 'default' periods of 90 days for technical assistance notices and 180 days for technical capability notices that do not specify an expiry date.)

However, the acts and omissions of the Director-General of Security (or delegate) in considering (or failing to consider) whether an assistance notice must be revoked would be subject to IGIS oversight as a matter of propriety, and could be a source of complaints to IGIS. The acts and practices of members of ASIO in bringing relevant information to the attention of the Director-General or

66 *ASIO Act,* subsections 29A(3) and 35F(5).

67 New sections 317R and 317Z.

68 Cf *ISA,* subsection 10(2A). This provision imposes a duty on *ISA* agency heads to inform their Minister if satisfied that the grounds for issuing a Ministerial authorisation no longer exist, and to take steps to discontinue the relevant activities. It also imposes a duty on the Minister to consider revoking the Ministerial authorisation. IGIS queries whether equivalent requirements could be applied to new s 317Z of the *Telecommunications Act* (revocation of technical capability notices by the Attorney-General); and similar requirements applied to agency heads under new s 317R (revocation of technical assistance notices).

delegate would similarly be subject to IGIS oversight. Similarly, ASIO's actions in providing advice or information to the Attorney-General about the existence of the grounds of revocation for a technical capability notice would also be the subject of IGIS oversight.

1.3.3 Are requests and notices intended to cover the repetitive provision of assistance? (New ss 317G, 317L and 317T)

Requests and notices apply to the doing of 'one or more specified acts or things' by a provider.[69] It is unclear whether requests and notices are capable of covering, and therefore immunising (and compelling in the case of notices) one or both of the following types of performance:

- the doing of a particular act or thing on a ***single occasion*** only, with the result that the request or notice (or a provision of the request or notice) is spent after the act or thing is done; or
- the provision of ***'standing assistance'*** comprising the ***repetition*** of a particular act or thing for the period of effect (or compliance period, if any) for the request or notice, with performance to occur upon the request or direction of the relevant agency, or at the discretion of the provider, or some combination.

Suggestion: statutory clarification of the intention in relation to 'standing assistance'

Clarification of the circumstances in which requests and notices can be used will be important to IGIS oversight of their use by ASIO, ASD and ASIS (as applicable). The potential for the repetition of requested or compelled assistance under a single request or notice will be particularly relevant to the oversight of agencies' assessment of proportionality-related matters in making issuing decisions, and decisions in specifying or nominating (as applicable) the expiry date for a request or a notice, in the absence of a fixed statutory maximum period of effect.

1.3.4 Provision of advice to designated communications providers

New subsections 317HAA(1)-(3) provide that if the Directors-General of ASIO, ASIS or ASD (or their delegates) give a technical assistance request, they must advise the relevant communications provider that compliance with the request is voluntary.

Suggestion: statutory form and timing requirements for advice

IGIS oversight of agencies' compliance with this requirement may be complicated by the absence of a statutory form requirement in relation to such advice, or a requirement that the advice concerning voluntary compliance must be given ***as part of*** a request given in writing or orally, ***and*** as part of a written record of an oral request. Such requirements would facilitate consistent record-keeping practices, and the subsequent oversight by IGIS of those records.

These observations also apply to the requirements in new subsection 317MAA(1) for the Director-General of Security to advise a communications provider about the effect of a technical assistance notice that has been issued by the Director-General.

69 New paragraph 317G(1)(a), new subsections 317L(1) and 317T(1).

1.3.5 The prohibition on creating 'backdoors' (new s 317ZG)

Limitations in the prohibition—no application to technical assistance requests

New section 317ZG prohibits a technical assistance or technical capability notice from requiring a provider to create a so-called 'backdoor' in the form of the introduction of a systemic weakness or vulnerability into a form of electronic protection.[70] It also prohibits these notices from preventing a provider from rectifying any existing 'backdoors' that it may identify.[71] These prohibitions also expressly cover obligations to build new decryption capabilities, and actions that would render existing systemic methods of authentication or encryption less effective.[72] Notices are of no effect to the extent that they purport to impose such requirements on a provider.[73]

No such prohibitions apply to technical assistance requests. This raises the legal possibility that ASIO, ASIS or ASD could negotiate an agreement with a provider to ***voluntarily*** create or fail to remediate a 'backdoor'. That provider would have civil immunity for doing so,[74] and would be taken to have been authorised for the purpose of the computer offences in Part 10.7 of the *Code*.[75] (For example, offences for causing unauthorised access to, or modification of, restricted data held in a computer under section 478.1 of the *Code*.)

While it is foreseeable that many providers would decline any such request because it is incompatible with their commercial and reputational interests, the possibility appears to exist that an individual provider could be persuaded to do so, and if so, compensated in accordance with a contract, agreement or other arrangement made under new section 317K.[76]

Suggestion: clarification of intended application
IGIS queries whether requests are intended to be utilised in this way, and would support clarification of the intended application.

If there is such an intention, any use of requests in this way would raise significant propriety risks, including in the assessment of the impacts of a 'backdoor' on the users of the relevant services, equipment or devices, whose information security may be unknowingly compromised. Employees or contractors of the communications providers may be prevented from disclosing this to users as result of the disclosure offences in new section 317ZF (among other potentially applicable secrecy offences, including those in the *ASIO Act, ISA* and new Division 122 of the *Criminal Code*).

---

70 New paragraph 317ZG(1)(a).

71 New paragraph 317ZG(1)(b).

72 New subsections 317ZG(2)-(4).

73 New subsection 317ZG(5).

74 New paragraphs 317G(1)(c) and (d).

75 New subparagraph 476.2(4)(b)(iv) of the *Code* (item 3 of Schedule 1 to the Bill).

76 It is also notable that the general principle in new section 317ZK that (unless otherwise agreed) a provider should neither profit from providing assistance, nor bear the reasonable costs of doing so, is limited to ***notices***. Contracts made under new section 317K in relation to ***requests*** are not subject to an equivalent requirement. Consequently, there is no apparent prohibition on contractual terms that would cause a provider to ***profit*** from providing assistance to an agency under a request, including a request to create or leave open a 'backdoor' in electronic protection. IGIS queries whether agencies' statutory contracting power should be subject to a limitation on making such contracts.

Further suggestion: statutory notification requirement in relation to requests for 'backdoors'

Given the level of risk involved in such activities, IGIS would support an express requirement for ASIO, ASD and ASIS to notify the Inspector-General (and their responsible Minister) of the making of technical assistance requests for a provider to create or fail to remediate a systemic weakness or vulnerability.

Challenges for independent oversight of compliance with new section 317ZG

In conducting oversight of ASIO's decisions to issue a technical assistance notice, or the terms of any request for the Attorney-General to issue a technical capability notice, IGIS will consider whether the notice or request to the Attorney-General complied with the limitations imposed by new section 317ZG.

The task of ascertaining whether a particular requirement under a notice amounted to a 'systemic' weakness or vulnerability may be extremely complex. The distinction between a 'systemic and a 'non-systemic' or 'selective' weakness or vulnerability may not always be clear, and is likely to require detailed assessments of fact and degree that are highly specific to the circumstances of individual cases, including the attributes of particular technologies and circumstances of their use. To some extent, the complexity of this task is acknowledged in the Explanatory Memorandum, which states that 'the nature and scope of any weakness or vulnerability will turn on the circumstances in question and the degree to which malicious actors are able to exploit the change required'.[77]

The degree of complexity of this task also appears to be reflected in the arrangements in new subsection 317W(7) as part of the consultation requirements if the Attorney-General intends to issue a technical capability notice. The Attorney-General and the provider who is the subject of the proposed notice may jointly appoint an expert to carry out an assessment of whether the proposed notice would contravene the limitations imposed by new section 317ZG. No equivalent mechanism applies to technical assistance notices.

Resource impacts for IGIS

The task of assessing ASIO's compliance with new section 317ZG will require a sophisticated understanding of a wide variety of communications and security technologies, including new and emerging technologies. One challenge for IGIS will be obtaining, within existing resources, necessary access to ***independent*** technical expertise to inform such assessments and to critically analyse ASIO's assessments and any information that may be provided by communications providers, and make an independent assessment.

It is presently unclear whether this need can feasibly be met from ordinary staffing. The extremely broad and rapidly changing range of technologies with which IGIS may need to have faculty may create a need for a level of expertise that exceeds what can reasonably be obtained 'in house'. The costs of engaging external consultants to act as specialist technical advisers may be prohibitive from within existing resourcing, if a need for such expertise is required regularly. This is contingent on ASIO's use of notices in practice, which is also contingent on a range of external factors.

77 Explanatory Memorandum, p. 68 at paragraph [258].

IGIS also notes that the issue of access by oversight bodies to independent technical expertise, particularly in relation to new and emerging technologies, may merit consideration in a more systemic way, including the potential for legislative frameworks and supporting administrative arrangements to ensure such access. (For example, the *Investigatory Powers Act 2016* (UK) establishes a Technology Advisory Panel to assist the Investigatory Powers Commissioner and the Secretary of State about the impact of changing technology on the exercise of investigatory powers conferred under that Act.)[78]

IGIS access to reports prepared under new subsection 317W(7)

In addition to the consideration of the resource implications of access to independent technical expertise, IGIS would be assisted by a mechanism to access to the expert reports prepared and given to the Attorney-General under new subsection 317W(7) for the purpose of the consultation obligations in relation to the issuing of technical capability notices.[79] Access to these reports would:

- offer a source of technical information to assist the Inspector-General's consideration of compliance with section 317G, in appropriate cases,[80] and to build an informed understanding of specific technologies and the impacts of the removal of certain forms of protection, while also operating within the strict secrecy and security requirements established under the *IGIS Act*;
- inform IGIS oversight of ASIO's requests to the Attorney-General for the issuing of technical capability notices. (That is, by comparing the case provided by ASIO to the Attorney-General about compliance with new section 317ZG with the findings in a report provided under new subsection 317W(7), if commissioned as part of the consultation requirements for that notice); and
- inform IGIS oversight of ASIO's decisions to issue a technical assistance notice that is related in some way to a technical capability notice already issued, and which was the subject of a report under new subsection 317W(7).[81]

78 *Investigatory Powers Act 2016* (UK), sections 246-247.

79 These reports may be commissioned from a person who has relevant expertise, who is appointed jointly by the Attorney-General and the communications provider to whom the proposed notice relates. They contain an assessment of whether a proposed technical capability notice would contravene section 317G. See further: new subsections 317W(7)-(11).

80 For example, if the same type of technology is the subject of a technical assistance notice issued by ASIO, or a request by ASIO for the issuing of a technical capability notice.

81 For example, this circumstance may arise if a technical capability notice compelled the provision of technical assistance to ASIO under new paragraph 317T(2)(b) and, after the expiry of that notice, ASIO decided to issue a technical assistance notice covering the same matter. It might also arise if a technical capability notice was issued to compel a provider to create or maintain a capability for the benefit of ASIO (or various agencies including ASIO) and ASIO subsequently issued a technical assistance notice to compel the provision of assistance using that capability. In both cases, if a report is provided under new subsection 317W(7), its findings on compatibility with new section 317ZG may be relevant to an assessment by IGIS of ASIO's actions in issuing a technical assistance notice or requesting the issuing of a technical capability notice (although the report would be not determinative of an independent finding by IGIS).

Suggestion: a statutory access provision for IGIS

IGIS supports consideration of a legislative mechanism to enable the provision of these reports, for example via an amendment to new section 317W or potentially an amendment to section 32A of the *IGIS Act* (which provides for the IGIS to have access to certain agency reports).[82]

1.4 Immunity from civil liability for acts done under a request or notice (new ss 317G(1)(b)-(d) and 317ZJ)

1.4.1 Scope of immunity

The immunity from civil liability for acts done in accordance with a technical assistance request or a technical assistance or capability notice is not subject to any express limitations or exclusions. For example, there are no exclusions for conduct that constitutes an offence; causes serious loss of, or damage to, property; or causes significant financial loss to another person.

This is in contrast with the proposed immunity in new subsection 21A(1) of the *ASIO Act* (in Schedule 5 to the Bill) for persons who provide voluntary assistance to ASIO, which contains specific limitations and exclusions.[83] The existing immunity from civil liability conferred on participants in ASIO's special intelligence operations also includes explicit limitations and exclusions.[84] The absence of limitations or exclusions on the proposed immunity in relation to technical assistance requests and technical assistance and capability notices must also be considered in the context of its breadth of application, covering the actions of the agents of a provider (as well as officers and employees) and things that are done in good faith in ***purported*** accordance with a technical assistance request or a technical assistance or capability notice.[85]

Suggestion: consistent statutory conditions and limitations on immunities in new Part 15

IGIS suggests that consideration is given to applying conditions and limitations on the immunities in new Part 15 of the *Telecommunications Act,* which are consistent with conditions and limitations on other immunities available to agencies (including agents and others assisting them); and with new subsection 21A(1) of the *ASIO Act* (subject to IGIS's comments at [5.1] below on the latter provision).

1.4.2 Absence of notification or reporting requirements about the use of the immunities

The Bill does not require ASIO, ASD or ASIS to keep any records of, or notify IGIS or their Ministers about, the use of the civil immunities conferred by the issuing of requests and notices. In the absence of such records, IGIS may obtain some visibility through complaints made by providers or third parties whose rights to obtain remedies are removed by the civil immunity, and through

82 This could include take the form of a requirement for IGIS to be notified of the provision of reports under new subsection 317W(7) and to provide a copy on request.

83 Schedule 5, item 2 (new paragraphs 21A(1)(d) and (e) of the *ASIO Act*). Note that IGIS has identified some possible unintended limitations in the conditions applying t the immunity in new subsection 21A(1) of the *ASIO Act*. (See [5.1] below.)

84 *ASIO Act,* paragraphs 35K(1)(d)-(e). Paragraph 35K(1)(f) also provides that the Attorney-General may by legislative instrument specify further requirements in a determination made under subsection 35K(2), and the availability of immunity is conditional on participants' compliance.

85 New subparagraph 317G(1)(b)(ii), new paragraphs 317G(1)(d) and 317ZJ(1)(b) and new subsection 317ZJ(3).

notification by agencies on a purely administrative basis. However, the receipt of individual complaints and administrative notification by agencies would not provide a reliable means for IGIS to develop an informed understanding of the circumstances in which the immunity is enlivened and its effects, and those instances in which the limits of the immunity are exceeded.

Suggestion: statutory reporting and notification requirements to IGIS

IGIS oversight of the exercise of the powers by intelligence agencies under new Part 15 would be significantly assisted by a requirement for agencies to report periodically to IGIS (and potentially their respective Ministers) on the use of requests and notices.[86] This would include instances that are known to ASIO, ASIS and ASD in which:

- a provider engaged in conduct in accordance or purported accordance with a request made by ASIO, ASIS or ASD (as applicable) or an assistance notice issued by ASIO, or a capability notice issued by the Attorney-General on the request of ASIO; and
- the provider's conduct caused significant loss of, or serious damage to, property; or significant financial loss; or
- the provider engaged in conduct in purported compliance with the request or notice that is excluded from the immunity. (For example, as a result of the limitations in new section 317ZH in relation to a notice.)

Such a requirement would, by extension, require ASIO, ASD and ASIS to take reasonable steps to obtain visibility of the acts and things done by providers in accordance with a request or notice, as applicable. This may be implemented by including conditions in requests or notices, or associated contracts. In any event, standards of propriety in relation to the making of requests or issuing of notices would require agencies to consider the likely impact of an immunity, and to have means to ensure that the conferral and application of that immunity remain proportional.

1.5 Immunity from criminal liability to certain computer offences (*Criminal Code*, new ss 476.2(4)(b)(iv)-(vi), item 3 of Schedule 1)

Item 3 of Schedule 1 to the Bill proposes to extend the 'authorisation' provision in Part 10.7 of the *Code*. The proposed amendments provide that a person who does an act or thing in accordance with a request or notice given under new Part 15 of the *Telecommunications Act* is taken to be entitled to cause access to or modification of data held in a computer; the impairment of an electronic communication to or from a computer; or the impairment of the reliability, security or operation of data held on an electronic data storage device.

The result is that the computer offences in Part 10.7 of the *Code*, in relation to causing unauthorised access, modification or impairment, do not apply to communications providers who engage in conduct that would otherwise constitute an offence under that Part, if they act in accordance with a request or notice.[87]

86 See also the comments below on the annual reporting requirements in new section 317ZS.

87 See especially the computer offences in sections 477.2, 477.3, 478.1 and 478.2 of the *Code*.

1.5.1 A broader immunity for providers than for intelligence agency staff and agents

As a matter of practicality, it is understandable that there is a desire to apply some form of limitation to the potential criminal liability of a communications provider who complies with a technical assistance or capability notice that purports to compel the provision of assistance.[88]

However, the proposed amendments in item 3 would seem to effectively confer an immunity on providers in relation to the computer offences in Part 10.7 of the *Code* that is considerably broader than the immunities available to staff members or agents of ASIO, ASD and ASIS.

In the case of ASIO

Members of ASIO are only taken to be authorised under section 476.2 of the *Code* if they act in accordance with a warrant issued by the Attorney-General.[89] ASIO's computer access warrants prohibit the doing of acts or things that are likely to materially interfere with, interrupt or obstruct the lawful use of a computer by any other person, unless necessary to do one or more of the acts or things authorised by the warrant.[90] These warrants also prohibit ASIO from doing any other act or thing that is likely to cause material loss or damage to a lawful user of a computer.[91]

Consequently, if ASIO were to exceed the limits of its authority under a warrant, the persons performing or directing the performance of the relevant acts or things under the warrant could be exposed to criminal liability under Part 10.7 of the *Code*.

No equivalent limitations would apply to the proposed authorisation of communications providers, where those providers act in accordance with an assistance request or notice issued by ASIO, or a capability notice issued by the Attorney-General on ASIO's request.[92]

In the case of ASD and ASIS

Staff members and agents of those agencies are only covered by the immunity in section 476.5 of the *Code* in relation to acts done outside Australia in the proper performance of their functions;[93] and certain preparatory acts done within Australia, provided that ASIO would not require a warrant to carry out those acts.[94]

---

88 Without a limitation on their exposure criminal liability under the computer offences in Part 10.7 of the *Code*, a provider could be simultaneously ***compelled*** by the notice to engage in the relevant conduct specified in the notice; and ***prohibited*** from doing so by the criminal law. It is not clear that the issuing of a notice under Part 15 of the *Telecommunications Act* would enliven the defence of lawful authority in section 10.5 of the *Code*.

89 *Code,* subparagraph 476.2(4)(b)(i).

90 *ASIO Act,* paragraph 25A(5)(a), subsection 27A(1) and paragraph 27E(5)(a). Further, the causation of material interference with, or interruption or obstruction of, the lawful use or a computer must be reported to the Attorney-General in warrant reports: *ASIO Act*, subsection 34(2). See [1.9] below.

91 *ASIO Act,* paragraph 25A(5)(b), subsection 27A(1) and paragraph 27E(5)(b).

92 As noted at [1.9] below, there are also no reporting requirements on the use of requests or notices by ASIO, ASD and ASIS (as applicable). This is in further contrast to sections 34, 34ZH and 35Q of the *ASIO Act* (reports by ASIO on special powers warrants, questioning and detention warrants and special intelligence operations) and section 10A of the *ISA* (reports by ASD and ASIS in relation to Ministerial authorisations).

93 *Code,* subsection 476.5(1).

94 *Code,* subsections 476.5(2) and 476.5(2A).

ASD and ASIS would also require a Ministerial authorisation if the acts were done for the purpose of (or purposes including) the production of intelligence on an Australian person; or in the case of ASIS would have a direct effect on an Australian person; or in the case of ASD, acts done for the purpose of (or purposes including) preventing or disrupting cybercrime undertaken or enabled by an Australian person.[95]

No equivalent limitations would apply to the proposed authorisation of communications providers for the purpose of Part 10.7 of the *Code*, in respect of acts or things done in accordance with a request made by ASD or ASIS.

1.5.2 Potential immunity for providers who comply with legally ineffective notices

The authorisation in item 3 may be capable of covering acts done in accordance with technical assistance and technical capability notices that have no legal effect under new section 317ZG or 317ZH of the *Telecommunications Act.*[96]

This possibility arises because Part 15 of the *Telecommunications Act* appears to distinguish between a notice (which is defined in new section 317B as a notice given under new section 317L or 317T); and the separate imposition of limitations on the legal effect of a notice (as applied by new sections 317ZG and 317ZH). This may leave scope for an argument that a notice which has no legal effect is still a 'notice' within the meaning of new Part 15 of the *Telecommunications Act*. The authorisation in item 3 does not contain any explicit qualification or exclusion in relation to notices that have no legal effect, and there may be scope for differing legal opinions about whether this is implied.

Suggestion: statutory clarification of intended effect

If there is no intention for item 3 to provide an authorisation in respect of compliance with a legally ineffective notice, then IGIS considers it would be preferable for this to be made explicit.

1.5.3 Immunity for providers in relation to voluntary acts in accordance with requests

It might also be questioned whether the authorisation in item 3 should treat ***voluntary compliance*** with a request in the same way as ***mandatory compliance*** with the requirements of a notice. In particular, new Part 15 of the *Telecommunications Act* does not expressly prohibit an agency from making a request of a provider to do the following acts or things, and thereby enlivening an effective immunity from criminal liability under Part 10.7 of the *Code* in favour of the provider:

- an act or thing that the agency could only do itself under a warrant or another type of statutory authorisation; or
- an act or thing that the agency ***could not*** be authorised to carry out under a warrant or authorisation, due to limitations or prohibitions on the acts capable of being authorised; or
- in the case of ASD and ASIS, an act or thing that would not be covered by the immunity in section 476.5 of the *Code* for ASD or ASIS staff members and agents. (For example because the act or thing was not done in the ***proper*** performance by the agency of its functions; or because

95 *ISA,* subparagraphs 8(1)(a)(i), (ii) and (iii).

96 That is, if a notice purported to compel a provider to do acts or things that would require a warrant or an authorisation and the conditions specified in new subsection 317ZH(4) did not apply; or if a notice purported to compel a provider to create, or to refrain from fixing, a 'backdoor'.

it was done in Australia and was not preparatory or ancillary to an act done outside Australia.) [97]

> Suggestion: a statutory limitation on the power of agencies to make requests
>
> Consideration might be given to expressly limiting the power of these agencies to make technical assistance requests, and limiting the scope of the authorisation in item 3 in relation to acts done in accordance with a request.
>
> Such amendments could align the effective immunity for providers with the limits of authority for ASIO, ASD and ASIS to engage in computer-related activities that would otherwise constitute offences under Part 10.7 of the *Code.*

1.5.4 Reporting on circumstances in which the immunity is enlivened

As per the suggestion **at [1.9] below** (reporting requirements) oversight would be aided by a reporting requirement for intelligence agencies in relation to their use of new Part 15 of the *Telecommunications Act*. This could usefully include a specific requirement for those agencies to report to the IGIS and their Ministers on each instance in which a communications provider engages in conduct pursuant to a request or a notice, and that conduct:

- engages the immunity from criminal liability to the Code offences in item 3 of the Bill; and
- causes material damage, material interference or material obstruction to a computer.

1.6 Attorney-General's procedures and arrangements for requesting technical capability notices (new s 317S)

New section 317S provides that the Attorney-General may, in writing, determine procedures and arrangements to be followed in the making of requests for the issuing of technical capability notices, which may include conditions to obtain the agreement of a person or body before making a request.[98]

IGIS would conduct oversight of ASIO's compliance with those procedures and arrangements in making requests for the issuing of capability notices (including requests made jointly with other agencies).[99] However, neither the Bill nor the existing provisions of the *IGIS Act* contain a

97 The making of requests by ASIO, ASD and ASIS in these circumstances would, however, raise matters of propriety in relation to the actions of that agency. There would be additional matters of legality in relation to any requests made by ASIS to a communications provider to provide assistance that had a direct effect on an Australian person. IGIS has taken the view that the requirements in subparagraphs 8(1)(a)(ib) and (ii) of the *ISA* for ASIS to obtain a Ministerial authorisation for such activities also apply to ***requests*** made by ASIS to ***other persons*** to undertake those activities. On this view, ASIS would need to obtain a Ministerial authorisation in order to make a technical assistance request in new section 317G of the *Telecommunications Act* in these circumstances. However, if ASIS did not obtain a Ministerial authorisation, an immunity from liability to computer offences in Part 10.7 of the *Code* would still be available to a communications provider who complied with that request, even though no such immunity would be available to ASIS staff members and agents under section 14 of the *ISA* or section 476.5 of the *Code* as a result of the breach of the Ministerial authorisation requirement.

98 New subsection 317S(1).

99 IGIS would also oversee ASIO's compliance with other requirements that may be specified by the Attorney-General under new section 317S, such as procedures contemplated in the Explanatory

mechanism to ensure that the Inspector-General is given a copy of the relevant documents, including variations.

In particular, the present obligations in section 32B of the *IGIS Act* on Ministers to give copies of directions and guidelines to the Inspector-General are limited to the responsible Ministers for intelligence agencies (which no longer includes the Attorney-General). Further, as determinations made under new section 317S are not legislative instruments[100] and could be classified, they may not be accessible via open source means. The absence of a statutory mechanism to facilitate timely access by IGIS to the latest versions of the Attorney-General's procedures and arrangements may complicate oversight of ASIO's compliance with requirements set down by the Attorney-General.

Suggestion: a statutory requirement to provide IGIS with procedures and arrangements

IGIS supports an amendment to new section 317S that requires the Attorney-General to give the Inspector-General a copy of all procedures and arrangements as soon as practicable after they are made.[101]

Consideration could also be given to a statutory requirement for copies of procedures and arrangements determined by the Attorney-General to be given to other integrity agencies with oversight responsibilities for the 'interception agencies' that may use the industry assistance scheme (such as the Commonwealth Ombudsman in relation to AFP and ACIC).

1.7 Terms and conditions on which help is to be given under a notice (new s 317ZK)

New section 317ZK sets out the key conditions upon which assistance is to be provided under a notice. These conditions include the general basis upon which a provider must comply with a requirements in a notice. (Namely, neither profiting from, nor bearing the reasonable costs of, compliance, unless the provider and agency otherwise agree.)[102] Other conditions include a default requirement for the parties submit to arbitration of the terms and conditions of compliance, if they cannot reach agreement.[103]

However, the Director-General of Security (or delegate) may decide to 'turn off' the statutory terms and conditions in new section 317ZK in relation to a requirement in a technical assistance notice issued by ASIO, if he or she is satisfied that the application of the section would be contrary to the public interest.[104] An equivalent power is conferred on the Attorney-General in relation to technical capability notices.[105] In determining whether it would be contrary to the public interest for new section 317ZK to apply, the decision-maker must have regard to several prescribed matters, including: the interests of law enforcement and national security; the objects of the

---

Memorandum, at p. 51, paragraph [145], to 'ensure that additional agencies are notified of requests being made'.

100 New subsection 317S(4).

101 Consideration could alternatively be given to amending section 32B of the *IGIS Act*.

102 New subsection 317ZK(3).

103 New subsection 317ZK(4).

104 New paragraph 317ZK(1)(c).

105 New paragraph 317ZK(e).

Telecommunications Act; the imposition of a regulatory burden on the provider; and the reasons for the giving of the notice.[106] The Bill does not contain a specific requirement for a provider to be notified of a decision to 'turn off' the application of section 317ZK in relation to them.

Existing Part 14 of the *Telecommunications Act* does not contain an equivalent power to 'turn off' the terms and conditions in section 314 in respect of the obligations on carriers, carriage service providers and intermediaries to give certain help to Commonwealth, State and Territory authorities under subsections 313(3) and 313(4).

1.7.1 IGIS oversight of the Director-General's power to 'turn off' new section 317K

IGIS is unlikely to have significant involvement in the oversight of ASIO's actions in costs negotiations in those cases in which the Director-General of Security (or delegate) ***does not*** decide to 'turn off' new section 317ZK. This reflects the availability of arbitration under that section.

However, decisions of the Director-General (or delegate) to 'turn off' new section 317ZK may be a source of complaints to IGIS by affected providers, in addition to potential complaints about disputed matters that would otherwise have been governed by the costs negotiation and arbitration provisions in new section 317ZK. Oversight of the actions of the Director-General or delegate under new section 317ZK will be assisted by the inclusive list of statutory factors that must be taken into account in assessing matters of public interest. However, complaints about decisions to 'turn off' new section 317K and underlying disputes about the apportionment of costs may have significant resource implications for IGIS.

1.7.2 Record-keeping in relation to decisions to 'turn off' new section 317K

It is important that IGIS has visibility of all decisions of the Director-General (or delegate) to 'turn off' the application of new section 317ZK to technical assistance notices issued by ASIO.

IGIS also notes that an assessment of some of the matters prescribed as mandatory considerations for public interest-based decisions to 'turn off' new section 317ZK may not be within ASIO's ordinary knowledge. (For example, the interests of law enforcement, and the assessment of the regulatory burden on the provider.) IGIS would examine the factual basis upon which the Director-General or delegate formed his or her views on those matters.

Suggestion: a statutory requirement for decisions to be made or recorded in writing

Ready access to written records of decisions, supporting reasons, and the information on which they are based, will be essential to such oversight. This could be facilitated through the imposition of a statutory requirement on the Director-General (or delegate) to record his or her decisions and the supporting reasons in writing.

106 New subsection 317ZK(2).

1.7.3 Complications in applying and overseeing decisions about the 'public interest test'

The power to 'turn off' new section 317ZK seems to apply collectively to ***all of the conditions*** in that section rather than individual conditions, such as the arbitration of certain matters. (In particular, as there is no requirement for decisions to 'turn off' new section 317ZK to be made ***by instrument***, the discretion in subsection 33(3A) of the *Acts Interpretation Act* may not be available.)[107]

If there is no ability to 'turn off' only ***some*** of the conditions in new section 317ZK in appropriate cases, this may complicate the application and oversight of the public interest test. In this event, it would be necessary for the decision-maker to make an 'aggregated' assessment of whether it would be contrary to the public interest for ***all*** of the conditions in new section 317ZK to apply to a requirement under a notice.

Suggestion: an explicit power to turn off only some conditions, and a power of deferral

IGIS questions whether provision could be made for greater flexibility in the exercise of the statutory power, so that the decision-maker is given discretion to decide to 'turn off' ***some*** of the conditions in appropriate cases; and could also decide to ***defer*** the availability of some conditions as a result of urgent circumstances (for example, until after a provider has performed its obligations under a notice) rather than to permanently exclude their application.

1.8 Disclosing information about requests and notices for oversight purposes (new s 317ZF)

New subsection 317ZF(1) applies various restrictions on the disclosure of information about the giving, existence, contents and performance of requests and notices, by various persons to whom that information is entrusted. Contravention of those restrictions is an offence.[108] However, new paragraph 317ZF(3)(f) and new subsection 317ZF(5) contain exceptions for disclosures to IGIS officials, and disclosures by IGIS officials, in connection with the performance by those persons of their functions or duties or the exercise of their powers as IGIS officials.

Subject to one issue (which is explained below), the exceptions in relation to IGIS officials are adequate to ensure that necessary information can be disclosed to, and by, IGIS officials for the purpose of conducting independent oversight of intelligence agencies' actions under the scheme. The provisions are generally consistent with the approach taken to exempting disclosures to and by IGIS officials from various secrecy offences that apply to the disclosure of sensitive information.[109]

---

107 Subsection 33(3A) of the *Acts Interpretation Act* relevantly provides that, where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character with respect to particular matters, the power is construed as including a power to make, grant or issue an instrument with respect to only ***some*** of those matters. (Courts have drawn a conceptual distinction between a power to ***issue an instrument***, which itself has an operative legal effect; and a power to ***make a decision*** which is immediately operative but, in the interests of good administration, is recorded in writing. See: *Laurence v Chief of Navy* (2004) 139 FCR 555 at 558 per Wilcox J.)

108 This is punishable by a maximum penalty of five years' imprisonment: new subsection 317ZF(1).

109 See, for example: *ASIO Act*, section 18D; *ISA*, subsection (3) of sections 39-40B and subsections (2A) of sections 40C-40M; and *Code,* subsection 122.5(3).

1.8.1 Imposition of evidential burden on IGIS officials (new subsection 317ZF(5))

The exception in new subsection 317ZF(5) (covering disclosures by IGIS officials) does not relieve an IGIS official from the requirement to discharge the evidential burden in respect of their status as an IGIS official, and the making of the disclosure in their capacity as an IGIS official.

In contrast, other exceptions to Commonwealth secrecy offences for disclosures of information by IGIS officials for the purpose of performing their official functions remove the evidential burden from the IGIS official as defendant in relation to these matters.[110] This recognises that current and former IGIS officials are under a legal disability as a result of the secrecy obligations and attendant offences in section 34 of the *IGIS Act*. These obligations are likely to prevent an IGIS official from adducing the evidence necessary to discharge the evidential burden in relation to the matters in new subsection 317ZF(5).

Suggestion: removal of evidential burden from IGIS officials

Accordingly, IGIS would support an amendment to new subsection 317ZF(5) bring it into alignment with the prevailing approach to equivalent provisions under other secrecy laws, including the official secrecy offences in Division 122 of the *Criminal Code* as enacted by the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (*EFI Act*).

1.8.2 Exceptions for disclosures to, and by, officials of other integrity agencies

IGIS queries whether further exceptions may be appropriate for disclosures to other integrity agencies (such as the Commonwealth Ombudsman and the Australian Commissioner for Law Enforcement Integrity) which have specific oversight functions in relation to some of the 'interception agencies' that may use the new industry assistance scheme (the AFP and ACIC).

Suggestion: alignment of exceptions with other Commonwealth secrecy offences

In addition to exceptions for disclosures to the Ombudsman and ACLEI, consideration might also be given to including exceptions for the making of public interest disclosures, disclosures to the Information Commissioner for the purpose of performing functions under freedom of information and privacy legislation, and the reporting of suspected offences or maladministration in the investigation of offences in connection with the new scheme.

This would bring the disclosure regime in new section 317ZF into line with the authorised disclosures for integrity related purpose in the official secrecy provisions in section 122.5 of the *Criminal Code* (as enacted by the *EFI Act*). Alignment of the exceptions may be desirable, as it would seem possible for a disclosure of information about a request or a notice to constitute a specific secrecy offence in Part 15 of the *Telecommunications Act* and a general secrecy offence in Division 122 of the *Code*.

110 See, for example: *ASIO Act,* section 18D; *ISA,* section 41B; and *Code,* section 122.5(12).

1.9 Reporting on intelligence agencies' use of new Part 15 (new s 317ZS)

The annual reporting requirements in new section 317ZS do not extend to the activities of ASIO, ASD and ASIS under new Part 15, as these reports are limited to the activities of 'interception agencies'.

In the experience of IGIS, reporting requirements about the exercise by intelligence agencies of intrusive and coercive powers significantly aid independent oversight. Reporting requirements are valuable because they mandate the consistent collection and maintenance of records, and the evaluation by the agency (and its Minister) of how each exercise of those powers assisted the agency to perform its functions. Reports also assist IGIS to:

- develop a comprehensive understanding of the way in which those powers are used;
- identify and analyse trends or patterns, including with respect to systemic issues; and
- compare the approaches of different agencies (where appropriate) including to identify best practice, or inconsistent practices not attributable to specific functions of individual agencies, or common compliance issues.

Suggestion: classified annual reporting requirements for intelligence agencies

While there may be security related arguments that the ***public*** annual reporting requirements in new section 317ZS should not apply to ASIO, ASD or ASIS, it is unclear why those agencies could not at least be subject to ***classified*** reporting requirements to their Ministers and IGIS in relation to their use of the scheme in new Part 15. Such reporting requirements could be included in agencies' classified annual reports.

Further suggestion: 'per request' and 'per notice' reporting for intelligence agencies

IGIS considers it important that there is also reporting on a 'per-request' or 'per-notice' basis, consistent with requirements in relation to ASIO warrants under section 34 the *ASIO Act* and Ministerial authorisations under section 10A of the *ISA*.

In particular, IGIS considers it important that intelligence agencies are required to inform their Minister and the Inspector-General in relation to conduct that engages the immunity from civil liability and the effective immunity from liability to the computer offences in Part 10.7 of the *Code,* where that conduct results in material loss, damage or harm to a third party, or material interference with or obstruction of the lawful use of a computer.

1.10 Incorrect references to the IGIS Act in the Explanatory Memorandum

IGIS notes that the commentary in the Explanatory Memorandum on Schedule 1 to the Bill contains some incorrect or misleading references to the *IGIS Act*. These references would benefit from correction to ensure that they do not mislead or confuse members of the public, including communications providers, about the independence of the office of the IGIS from the National Intelligence Community that it oversees.

In relation to the conditions for making technical assistance requests under new paragraph 317G(5)(d), the Explanatory Memorandum states that this provision 'reflects the functions of

Australia's intelligence and security agencies as set out in the ***IGIS Act*** and the *ASIO Act*'.[111] The reference to the *IGIS Act* may have been intended to be a reference to the *ISA*. IGIS is not part of the National Intelligence Community, and will not be conferred with any powers under new Part 15 of the *Telecommunications Act*. These matters are important to public confidence in the independence of IGIS, including the over sight of the actions of ASIO, ASIS and ASD under Part 15.

In relation to compliance and enforcement measures in Division 5 of new Part 15, the Explanatory Memorandum cites the *IGIS Act* as part of the justification for the non-merits reviewable status of technical assistance and capability notices. It states that the exclusion of merits review of decisions made under new Part 15 is 'consistent with other decisions made for national security and law enforcement purposes—for example those made under the *IS Act*, *ASIO Act*, ***IGIS Act*** and *TIA Act*. Decisions of a law enforcement nature were identified by the Administrative Review Council in its publication *What decisions should be subject to merits review?* as being unsuitable for merits review'.[112] The reference to the *IGIS Act* in this context may create a misleading impression that IGIS is a security or intelligence agency akin to those agencies which are governed by the other Acts listed (such as ASIO, ASIS and ASD), or is a law enforcement agency, or will otherwise be conferred with powers under new Part 15 of the *Telecommunications Act*.[113]

Schedule 2—ASIO's computer access warrants

Schedule 2 to the Bill proposes to amend ASIO's warrant-based computer access powers (in sections 25A, 27A and 27E of the *ASIO Act*). The key amendments will permit ASIO to:

- undertake telecommunications interception (TI) for the purpose of doing any thing that is specified in the warrant, including but not limited to accessing relevant data held on, or from, a computer;[114]
- temporarily remove a computer or other thing from premises, for the purpose of doing any thing specified in the warrant;[115] and

111 Explanatory Memorandum, p. 45 at paragraph [99].

112 Explanatory Memorandum, p. 60 at paragraph [207].

113 Further, the reason that the decisions of the IGIS are not merits reviewable is their connection with the making of ***advisory recommendations*** to the ultimate decision-maker (being the responsible Minister, Prime Minister or Attorney-General). See further: Administrative Review Council, *What Decisions Should be Subject to Merit Review*, 1999 at [4.44]-[4.48] ('recommendations to ultimate decision-makers'). This ground was identified as wholly separate to the potential exclusion from merits review of decisions concerning national security, the latter being recognised as a type of 'policy decision of a high political content' at [4.23]. Decisions of IGIS are clearly not of a political nature or content (being advisory recommendations of an independent oversight body, whose mandate is to examine the legality and propriety of intelligence agencies' actions).

114 Items 6 and 11: new paragraphs 25A(4)(ba) (computer access warrants) and 27E(2)(ea) (computer access authorisation under identified person warrants). Note that the power in new paragraph 25A(4)(ba) will be applied to foreign intelligence warrants by existing subsection 27A(1).

115 Items 5 and 10: new paragraphs 25A(4)(ac) (computer access warrants) and 27E(2)(da) (computer access authorisation under identified person warrants). Note that the power in new paragraph 25A(4)(ac) will be applied to foreign intelligence warrants by existing subsection 27A(1).

- undertake certain activities (including TI and temporary removal of computers and other things) to conceal the fact that any thing was done under a warrant, for up to 28 days after the warrant ceases to be in force, or as soon as reasonably practicable after the 28-day period.[116]

As a general observation, clarity on the face of the statute is particularly important in the context of ASIO's warrants, in terms of facilitating compliance by ASIO and independent oversight by IGIS of ASIO's actions. Unlike most law enforcement warrants, decisions about the issue and exercise of powers under these warrants are unlikely to be litigated, given that they are normally covert to the target and others. Consequently, there is likely to be limited, if any, opportunity for the judicial determination of the meaning of ambiguous provisions.

2.1 Telecommunications interception powers

2.1.1 No requirement to particularise telecommunications services or persons

The amendments in Schedule 2 will not require a warrant under section 25A or 27A, or an authorisation under section 27E, to particularise any telecommunications services or persons (by reference to their use of a service or a device) in respect of which interception is authorised. This is in contrast with requirements for TI warrants issued to ASIO under Part 2-2 of the *TIA Act*.[117]

The absence of such a requirement may reflect an intention that the primary statutory limitation on interception carried out under a computer access warrant is the purpose for which that interception may be conducted. That is, the purpose of doing any thing specified in the warrant in accordance with subsection 25A(4) and equivalent provisions in sections 27A and 27E (as amended) rather than which service is intercepted for that purpose.

Nonetheless, the absence of a requirement to specify telecommunications services or persons will further expand the powers available to ASIO under its computer access warrants. These powers are already broad, including as a result of the definition of a 'computer',[118] the 'security matter'[119] or 'foreign intelligence matter'[120] in respect of which warrants can be issued, and the applicable issuing thresholds.

---

116 Items 7, 8 and 12: new subsections 25A(8) (computer access warrants), 27A(3C) (foreign intelligence warrants) and 27E(6) (authorisation under identified person warrants).

117 *TIA Act*, sections 9, 9A, 11A and 11B. See also the condition for the issuing of a section 11C warrant that a section 11A or 11B warrant would be ineffective: subparagraph 11C(1)(b)(iii).

118 *ASIO Act,* section 22. (A 'computer' means all or part of one or more computers, computer systems, computer networks or any combination of these.)

119 *ASIO Act*, subsection 25A(2). (This is the matter that is important to security, in respect of which the warrant is issued. A 'security matter' could be defined very broadly, to cover legal and natural persons including bodies politic, entities or other things such as activities or events, and would not necessarily require the relevant matter to be known, in the sense of the identification of a particular person or entity, or a specific activity or event.)

120 *ASIO Act,* paragraph 27A(1)(a). (This is a matter specified in a notice given to the Attorney-General, as the purpose for which the foreign intelligence collection warrant is issued. For a warrant to be issued, the Attorney-General must be satisfied, on the basis of advice from the Defence Minister or Foreign Minister, that the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, foreign relations or economic well-being. As with a 'security matter' the 'foreign intelligence matter' could be very broadly defined to cover natural and legal persons, including bodies politic, entities or other things such as activities or events.)

Even taking into account the anticipatory nature of intelligence collection activities under ASIO's special powers warrants, the result is that the exercise of TI powers might be authorised on a much broader scale than may be immediately apparent on the face of the provisions, and on a broader scale than would be permitted under the *TIA Act.*

This circumstance will be relevant to IGIS oversight of the information that ASIO provides to the Attorney-General about the proposed collection activities in its warrant requests. In particular, it will be relevant to IGIS oversight of ASIO's decision-making about whether to request the issuing of a warrant with specific conditions that limit interception to particular services or persons; and the information that ASIO provides to the Attorney-General about its consideration of this matter.

2.1.2 Scope of interception activities authorised

The amendments will authorise TI for the purpose of doing any thing specified in the warrant, in accordance with the list of things that the Attorney-General may specify under subsections 25A(4), 27A(1) or 27E(2) (as amended).[121] IGIS understands that the amendments are intended to remove the need for ASIO to obtain two warrants (one authorising computer access and the other authorising TI) to conduct computer access and network exploitation activities.[122] The proposed powers may be framed more broadly than what is necessary to achieve this intended outcome.

Authorisation of TI to do any of the things in subsection 25A(4) as specified in the warrant

TI can be authorised for the purpose of doing any of the things in subsection 25A(4) or 27E(2). However, not all of the acts or things specified in subsections 25A(4), and 27E(2) are directly connected with ASIO obtaining access to 'relevant data'[123] that is held in, or is accessible from, a computer. For example, under the amendments as presently drafted, it would be open to the Attorney-General to authorise TI for the purpose of ASIO gaining entry to premises under paragraphs 25A(4)(aa) and (aaa) and equivalent provisions in subsections 27A(1) an 27E(2). It is unclear whether the conferral of such power is intended.

Suggestion: limitation of the TI power to a subset of things specified in the warrant

Consideration could be given to limiting the TI power to a ***subset*** of the things specified in subsections 25A(4) and 27E(2) such as the acts done for the purpose of accessing relevant data under paragraphs 25A(4)(a)-(ab) and 27E(2)(c) and (d).

Implications of the scope of the proposed TI power

The circumstances in which TI powers might be thought necessary to gain entry to premises are not immediately apparent. (Is this power intended to, for example, authorise the interception of communications sent and received by a known occupier or user of premises, in order for ASIO to ascertain their movements and activities at a particular time and therefore ensure that entry could

121 See also the authorisation of TI for concealment purposes in items 7, 8 and 12: new paragraphs 25A(8)(h), 27A(3C)(h) and 27E(6)(h) including after the expiry of the warrant.

122 Explanatory Memorandum, p. 80 at paragraphs [352]-[355].

123 See: *ASIO Act*, paragraph 25A(4)(a), subsection 27A(1) and paragraph 27E(2)(c). ('***Relevant data'*** is data that is relevant to the security or foreign intelligence matter in respect of which the warrant is issued; or in the case of identified person warrants, data that is relevant to the prejudicial activities of the identified person).

be made covertly? Could it authorise TI for the purpose of disabling, or using, a security surveillance system installed on the premises, noting that commercially available surveillance products commonly have internet or cellular connectivity?)

The conferral of TI powers for the purpose of gaining entry to premises would also result in different powers being available to ASIO to gain access to premises under a computer access warrant, as compared to other types of special powers warrants that authorise access to premises, such as search warrants and surveillance device warrants.

In practical terms, the breadth of the TI powers proposed to be conferred under ASIO's special powers warrants is also relevant to the subsequent use that could be made of intercepted information in reliance on new subsection 63AC(2) of the *TIA Act* (item 124 of Schedule 2 to the Bill).

In particular, new paragraph 63AC(2)(f) of the *TIA Act* would authorise the subsequent use of intercepted communications for purposes ***other than*** doing the things authorised by a computer access warrant, if their content related, or appeared to relate, to the involvement, or likely involvement, of a person in activities that are, or are likely to be, a threat to security (within the meaning of that term in section 4 of the *ASIO Act*).

IGIS notes that the broader the purposes for which TI powers may be exercised under a computer access warrant, the greater the practical likelihood that the contents of intercepted communications may contain information that is not relevant to the particular purpose for which the interception was carried out. This may, in turn, increase the practical likelihood that ASIO will make secondary use of those communications in accordance with new subsection 63AC(2) of the *TIA Act*, rather than obtaining a separate interception warrant under the *TIA Act* to undertake the interception.[124]

Application of 'use of force authorisation' in ss 25A(5A)(a), 27A(2)(a) and 27J(3)(d)

Existing paragraphs 25A(5A)(a), 27A(2)(d) and 27J(3)(d) provide that a computer access warrant, a foreign intelligence warrant, or an authorisation under an identified person warrant ***must authorise*** the use of any force against persons and things that is reasonably necessary to do the things specified in the warrant (or in an authority under an identified person warrant). Therefore, if a warrant authorises ASIO to carry out TI as a result of the amendments in Schedule 2 to the Bill, that warrant ***must*** authorise ASIO to use force against things and persons for the purpose of TI (as well as any other activities authorised under the warrant).

As interception warrants issued under Part 2-2 of the *TIA Act* do not authorise the use of force, this is an extension of powers available to ASIO, and not merely the relocation of an existing TI power into a different Act. It is unclear if the use of force against a person or thing could ever be necessary or reasonable to intercept a telecommunication under a warrant, however, the proposed amendments create the possibility for such an assessment to be made.

---

124 Cf the statement in the Explanatory Memorandum, at p. 15, paragraph [54], that 'ASIO can only use intercepted information in order to execute the computer access warrant. In order for ASIO to use intercepted information for its own intelligence value, ASIO must obtain an interception warrant under the *TIA Act*'. No reference is made to the effect of new subsection 63AC(2) of the *TIA Act* with respect to the secondary use of this information, including the effect of the broad exception in new paragraph 63AC(2)(f) for information that relates, or appears to relate, to the involvement of a person in activities that are, or are likely to be, a threat to security (within the meaning of that term in the *ASIO Act*).

Suggestion: possible exclusion of TI from the 'use of force' authorisation

If there is no intention to require warrants to authorise the use of force for the purpose of TI, consideration could be given to amending subsection 25A(5A) to exclude TI activities from the mandatory authorisation for the use of force.

If there is an intention to authorise ASIO to use force against persons or things for the purpose of carrying out TI, this would be subject to the requirement in section 31A for ASIO to notify IGIS, in writing, as soon as practicable if force is used against a person. IGIS would examine such activities closely, as well as ASIO's training and internal authorisations for the use of force potentially available in the exercise of TI powers.

2.1.3 Warrant reports

Schedule 5 to the Bill does not make a consequential amendment to the reporting requirements for special powers warrants under section 34 to impose a specific obligation on ASIO to report on the ***interception activities*** that are conducted under a computer access warrant.

This means that interception activities carried out under a computer access warrant will be subject to less detailed reporting requirements than for interception activities conducted under an interception warrant issued under Part 2-2 of the *TIA Act*. Section 17 of the *TIA Act* relevantly requires warrant reports to specifically address how ***each interception activity*** carried out under an interception warrant assisted ASIO in performing its functions. These reports must also include particulars of the telecommunications service or services to or from which each intercepted communication was made under named person warrants in sections 9A and 11B. In contrast, section 34 requires ASIO to report on the extent to which the action taken under the warrant assisted ASIO in carrying out its functions. This does not require the same particularisation of interception activities as section 17 of the *TIA Act*.

Suggestion: alignment of reporting requirements with the TIA Act

Oversight of the extended computer access warrant powers would be enhanced if reports on computer access warrants prepared under section 34 of the *ASIO Act* were required to address the same matters as those in section 17 of the *TIA Act* with respect to interception activities.

2.2 Temporary removal of computers and other things from premises

The new temporary removal powers are exercisable during and after the expiry of a warrant, for the purpose of doing ***any thing*** specified in the warrant, in accordance with subsections 25A(4), 27A(3C) and 27E(2).[125]

2.2.1 Purpose of temporary removal

The Explanatory Memorandum identifies that the temporary removal power is intended to be used in 'situations where ASIO may require specialist equipment, which cannot be brought onto the premises in a covert fashion, ***in order to access the computer***' (emphasis added).[126] However, the

125 See also the temporary removal powers for the purpose of concealment in items 7, 8 and 12: new paragraphs 25A(8)(f), 27A(3C)(f) and 27E(6)(f).

126 Explanatory Memorandum, p. 79 at paragraph [348].

proposed amendments would be capable of authorising temporary removal for broader purposes than obtaining access to relevant data that is held in, or is accessible from, a computer. This is because the activities that may be authorised under a computer access warrant in subsections 25A(4) and 27E(2) cover a broader range of activities, including gaining access to premises. As with the earlier observations on TI powers, consideration might be given to whether the temporary removal power could be limited to a subset of matters in subsections 25A(4) and 27E(2).

2.2.2 Meaning of 'other things' that may be temporarily removed

In addition to the temporary removal of computers from premises, computer access warrants will be able to authorise the temporary removal of 'other things' from premises. There is ambiguity in the meaning of these words. This may complicate oversight of the removal of things other than computers from premises that are accessed under the warrant.

In particular, could the removal power authorise the removal of ***any object*** on the premises for the purpose of doing an act or thing authorised in the warrant? It is arguable that the meaning of the words 'or other thing' should be construed by reference to the preceding word 'computer' and the broader context of the words 'or other thing' in a provision whose purpose is to authorise computer access. On this interpretation, the 'other thing' would need to have a rational connection with a computer. (For example, a data storage device, such as an external hard drive or media drive, which operates in conjunction with a computer.) Even if the words 'other thing' were given a narrow interpretation, there may be uncertainty as to whether a particular thing had the requisite nexus with a computer.

Suggestion: statutory clarification of the 'other things' that can be removed temporarily

In view of the above ambiguity, the temporary removal provisions could usefully provide greater clarity about the 'other things' that can be removed under a computer access warrant.

2.2.3 Duration of temporary removal

Temporary removals of computers or other things from premises under computer access warrants are a potential source of complaints to IGIS, given that most people make significant use of computers in conducting their business and personal affairs. The removal of a computer from premises could have severe impacts on its owner and other users, who may be prevented from making essential communications, conducting lawful business and deriving an income for the period of removal.

The amendments do not specify a maximum period of time during which computers and 'other things' may be removed from premises before they must be returned. Nor is there a statutory requirement to return a computer or other thing that is removed as soon as reasonably practicable. The result appears to be that the amendments could authorise the removal of a computer or any other thing from premises for an open-ended (and potentially protracted) period.

Suggestion: alignment with statutory conditions for temporary removal under search warrants

Consideration could be given to inserting a statutory condition on the duration of removals and the return of computers or things to premises.

For example, existing subsections 25(4C) and 27D(5) (in relation to search warrants and search authorisations under identified person warrants) provides that a record or any other thing that has been removed from the subject premises or from a person at or near the premises may be retained for only such time as is reasonable. If returning the record or thing would be prejudicial to security, then it may only be retained until its return would no longer be prejudicial to security. (However, this may still be a substantial period of time, and could enable indefinite retention if it is determined that return at ***any time*** would be prejudicial to security.)

2.2.4 Absence of reporting requirements for temporary removals

The Bill does not propose to amend the warrant reporting requirements in section 34 to require reports on computer access warrants to identify whether a computer or other thing was removed from premises, and if so, the purpose and duration of the removal. Reporting may be triggered under existing subsection 34(2) if a removal causes material interference with, or interruption or obstruction of, the lawful use of a computer by another person. However, as outlined below, there is ambiguity as to whether this would cover ***all instances*** of removal, and this ambiguity may lead to inconsistent interpretations, and therefore inconsistent reporting practices.

Suggestion: specific reporting requirement for all removals

The absence of a specific reporting requirement for ***all removals*** may also mean that that suitably detailed records may not be made (or may not be made consistently) of the reasons for, and duration of, each removal, which would make oversight difficult. Consequently, IGIS would support a statutory reporting requirement for all removals.

This would also help to alleviate complexity in relation to the application of reporting requirements concerning temporary removals that cause material interference, interruption, obstruction or loss or damage (discussed at [2.2.5]-[2.2.7]below).

2.2.5 Temporary removal and the existing limitation on acts that are likely to materially interfere with, interrupt or obstruct the lawful use of a computer

It is conceivable that the removal of a computer from premises could amount to the doing of a thing that is likely to materially interfere with, interrupt or obstruct the lawful use of that computer by other persons. (That is, the removal would necessarily deprive the owners and any other users of the computer of the opportunity to use it for the period of removal.)

Given the centrality of computers to the conduct by most persons of their ordinary, lawful business and personal affairs, that deprivation could reasonably be regarded as likely to be a ***material*** interference with, or a material interruption or obstruction of, their lawful use of the computer in many cases. In this event, the limitation in existing paragraph 25A(5)(a), and equivalent provisions applying to sections 27A and 27E, would apply. The removal may only be effected if it is ***necessary*** (and not merely convenient or useful) to do the thing authorised under subsection 25A(4) for which the computer was removed from the premises.

ASIO would need to make an assessment, in the circumstances of each proposed removal, of whether a person would be deprived of the use of a computer, and if so whether the condition of necessity is met. This is likely to be complex for ASIO to assess and for IGIS to oversight. Nonetheless, IGIS would expect to see evidence of an assessment of these matters in the course of ASIO's decision-making about the exercise of a temporary removal power. This oversight would be assisted by a standing reporting requirement for all temporary removals, noted above.

2.2.6 Temporary removal and the existing prohibition on acts that are likely to cause material loss or damage to persons lawfully using a computer

Existing paragraph 25A(5)(b) (and equivalent provisions applying to sections 27A and 27E) would have the effect that the removal of a computer or any other thing from premises would not be authorised if, in the circumstances, the removal is likely to cause any other material loss or damage to other persons lawfully using a computer.

This would seem to cover the risk of physical damage caused by the removal and return of a computer or in operating other equipment to gain access to the relevant data held on, or accessible from, that computer when it has been removed. It could also cover economic loss sustained by a user of the computer as a result of being deprived of its use or functionality for the period of removal. For example, if a computer was a business asset from which a person derived an income.

Paragraph 25A(5)(b) (and equivalent provisions applying to sections 27A and 27E) is an absolute prohibition. IGIS would therefore pay close attention to ASIO's assessment of the likelihood of such loss or damage in its decision-making about whether to exercise a temporary removal power.

2.2.7 Application of the existing reporting requirements in subsection 34(2) to temporary removals of computers and other things from premises

Existing subsection 34(2) will require ASIO to report on exercise of a removal power if the removal causes material interference with, or obstruction or interruption of, the lawful use of a computer, other electronic equipment or a data storage device. (For example, if the removal deprived a person of the ability to use the computer, or if the computer is damaged during its removal or return.)

The amendments to subsection 34(2) made by items 14 and 15 of Schedule 2 to the Bill will also extend the reporting requirement to material interference, obstruction or interruption caused by a temporary removal under the concealment powers in new subsections 25A(8), 27A(3C) and 27E(6).

However, it may be difficult to accurately identify whether temporary removal, in fact, deprived a person an opportunity to lawfully use a computer or other thing during the period of removal, and if so, the effects of the removal on the person.

Such difficulty may tend in support of amending section 34 to include an additional reporting requirement for ***all instances*** of removal **(as suggested at [2.2.4] above).** Without such a reporting requirement, IGIS would have limited practical capacity to know the frequency with which computers and other things are removed from premises, and to use this information to independently examine ASIOs actions and broader risk-management practices in relation the exercise of the new warrant-based removal powers.

2.2.8 Differences in the temporary removal powers applying to search warrants

The amendments in Schedule 2 that confer removal powers in connection with computer access warrants are drafted differently to the existing powers under search warrants (and authorisations under identified person warrants) that may authorise the removal of computers from premises.[127] Differences in the drafting of the individual provisions applying to different warrants may create a risk that the respective removal powers could be subject to different interpretations.

> **Suggestion: possible alignment of search warrant provisions**
>
> It may be desirable for the Bill to make some amendments to sections 25 and 27D, if there is a desire for consistency in all of ASIO's warrant-based computer removal powers.

In particular, the power of removal in relation to search warrants (and search authorisations under identified person warrants) applies generally to 'records' and 'other things' found on the premises (or on a search of a person at or near the premises) for the purpose of 'inspecting' or 'examining' those records or things.[128] The powers to use computers, equipment and devices found on, or brought to, the subject premises to access relevant data are authorised separately to the removal power.[129] The consequences of this separation include the following:

- the temporary removal power is not linked explicitly to the purpose of exercising the separate powers to use a computer, equipment or device;[130]
- there may be scope for doubt as to whether the existing purposes of removal (being 'inspection' or 'examination') could cover certain computer-related activities specified in the separate powers to use computers, such as: the conversion or copying of relevant data; and adding, copying, deleting or altering other data for the purpose of accessing relevant data;[131]
- the statutory limitations on causing material interference, interruption, obstruction, loss or damage to lawful users of the computer, equipment or device are expressed as applying to the powers to ***use*** those items (and no mention is made of the separate power of removal for the purpose of examination);[132] and
- the reporting obligation under subsection 34(2) in relation to search warrants is also expressed as applying to the causation of material interference, interference, obstruction, loss or damage

---

127 *ASIO Act,* ss 25(4)(d), 25(4A)(c) and 25(4C)-(6) (search warrants); and ss 27D(2)(g)-(i) and 27D(5) (authorisation to search premises and persons under identified person warrant).

128 *ASIO Act,* ss 25(4)(d)(i) and 25A(4A)(c)(i); and 27D((2)(g)(i).

129 *ASIO Act,* ss 25(5)-(6); and 27D(2)(h)-(k) and 27D(6)-(7).

130 Cf proposed ss 25A(4)(ac) (item 5) and 27E(2)(da) (item 10) which authorise temporary removal for the purpose of doing any thing under subsection 25A(4) or 27E(2), which includes using a computer or other things to access relevant data under existing ss 24A(4)(a) and (ab) and 27E(2)(c) and (d).

131 The amendments made in items 5 and 10 of Schedule 2 to the Bill could create or enlarge doubt. It might be argued that the presence of an express reference to these activities as a purpose of removal in ss 25A and 27E, and the absence of an express reference in ss 25(4), 25(4A) and 27D(2), might evince an intention for the latter (search-related) powers to be interpreted differently.

132 *ASIO Act,* ss 25(6) and 27D(7) which apply specifically to acts done under ss 25(5) and 27D(2)(h)-(k). Cf ss 25A(5) and 27E(5) which apply to all of the acts authorised under ss 25A(4) and 27E(2).

in connection with the exercise of the powers to ***use*** a computer, equipment or device (and no reference is made to the separate removal power).[133]

2.3 Concealment of acts or things done under a computer access warrant

Schedule 2 to the Bill proposes further amendments to the *ASIO Act* to insert new subsections 25A(8), 27A(3C) and 27E(6).[134] These provisions authorise specified concealment activities at any time while the warrant is in force, and up to 28 days after its cessation (or at the earliest time that is reasonably practicable after that 28-day period).

In addition to authorising ASIO to do any thing that is reasonably necessary to conceal the doing of an act or thing under a warrant, the concealment-related powers include: entry to premises; the temporary removal and return of computers or other things from premises; the use of other computers or communications in transit; the interception of telecommunications; and other things reasonably incidental to these activities. There is no requirement for the Attorney-General to specifically authorise any or all of these concealment activities in individual warrants. Rather, all computer access warrants are taken to authorise these activities.

2.3.1 Interaction of existing concealment powers with the new concealment powers

There appears to be uncertainty in the relationship between the proposed concealment powers in new subsections 25A(8) and 27E(6), and the existing concealment powers in paragraphs 25A(4)(c) and 27E(2)(f). The existing provisions enable the Attorney-General (or the Director-General in the case of section 27E) to authorise the doing of any thing that is reasonably necessary to conceal the fact that a thing has been done under the relevant warrant. Such activities must be specifically authorised in each warrant, and that authorisation is only in force for the duration of the warrant.

Consequently, there is overlap between the concealment activities that are authorised under new subsections 25A(8) and 27E(6) ***while the warrant is in force***, and the concealment activities that may be authorised by the Attorney-General under existing paragraph 25A(4)(c) and the Director-General or the Attorney-General under existing 27E(2)(f) during the same period.

Suggestion: removal of overlap of existing and new concealment powers

As it is difficult to envisage how the two sets of provisions could operate concurrently, it may be simpler for existing paragraphs 25A(4)(c) and 27E(2)(f) to be repealed, so that concealment is governed solely by new subsections 25A(8) and 27E(6).

2.3.2 No limitation on concealment activities likely to cause 'material interference' or 'material loss or damage' to lawful computer users

The concealment-related powers in new subsections 25A(8), 27A(3C) and 27E(6) do not appear to be subject to equivalent limitations and prohibitions to those in existing subsection 25A(5) (and corresponding provisions applying to sections 27A and 27E) in relation to acts that are likely to materially interfere with, interrupt or obstruct the lawful use of a computer by any person; or cause material loss or damage to lawful users of a computer.

133 *ASIO Act,* s 34(2)(b).

134 Items 7, 8 and 12.

The limitations and prohibitions in subsection 25A(5) (and equivalent provisions in sections 27A and 27E) only apply to things that are ***authorised under*** subsection 25A(4) (and equivalents). Hence, the limitations in subsection 25A(5) would only apply to an authorised concealment activity during the life of the warrant that is authorised under existing paragraph 25A(4)(c), and incidental matters under paragraph 25A(4)(d). This gap may be unintended.

Suggestion: an equivalent limitation on the concealment powers to that in s 25A(5)

Consideration could be given to amending the concealment powers in new subsections 25A(8), 27A(3C) and 27E(6) to include an equivalent limiting provision to that in existing subsection 25A(5).

2.3.3 Reporting on concealment activities carried out after the expiry of a warrant

Item 16 of Schedule 2 amends the reporting requirement in section 34 of the *ASIO Act* to provide that actions taken under the concealment provisions in new subsections 25A(8), 27A(3C) and 27E(6) is taken to have been done under the relevant warrant (namely, the computer access, foreign intelligence or identified person warrant).

A reporting requirement on concealment activities that are undertaken after the expiry of the warrant will assist oversight of those activities. However, the consolidation of a reporting requirement for 'post-warrant' concealment activities with the requirement to report on activities undertaken ***during*** the period of the warrant may unintentionally create delay in the making of warrant reports. As there is no maximum period of time during which 'post-warrant' concealment activities may be carried out after the warrant has expired, it is possible that such activities may be undertaken a considerable period of time after the warrant has ceased to have effect.

Suggestion: a separate reporting requirement for 'post-warrant' concealment activities

To facilitate the timely provision of warrant reports under section 34, consideration could be given to the inclusion of separate reporting requirements for concealment activities that are carried out (or are continuing to be carried out) later than 28 days after the expiry of the warrant, in reliance on the post-warrant concealment powers in new subsection 28A(8), 27A(3C) or 27E(6), as applicable.[135]

135 IGIS acknowledges that no separate reporting requirements currently apply to activities carried out under existing subsection 26B(5) to retrieve a surveillance device, and conceal the retrieval activity, after the expiry of the relevant surveillance device warrant. However, activities to conceal the retrieval of a surveillance device are of a materially different character to the activities involved in the concealment of access to a computer. The latter may require different actions, over time, to initially conceal and thereafter continue to conceal access.

2.4 Disclosures of 'ASIO computer access intercept information' to IGIS

The Bill proposes to amend Part 2-6 of the *TIA Act* (permitted dealings with intercepted information) to create a new concept of 'ASIO computer access intercept information' that covers TI information obtained under a special powers warrant authorising computer access.[136]

The Bill proposes to amend paragraph 64(1)(a) of the *TIA Act* to exclude 'ASIO computer access intercept information' from the permitted uses and disclosures of intercept information in connection with ASIO's functions, and the performance by IGIS of her functions.[137]

The Bill also proposes to insert new section 63AC, which authorises permitted dealings with 'ASIO computer access intercept information'.[138] However, new section 63AC only prescribes permitted dealings in relation to 'ASIO computer access intercept information' for the purpose of doing things that are authorised by an ASIO computer access warrant, or in other prescribed circumstances, which are generally directed to security and safety related purposes. They ***do not*** cover the performance by IGIS of oversight functions.[139]

2.4.1 Possible unintended omission of an exception for disclosures to and by IGIS officials

IGIS assumes that this is an unintended result.[140] Its effect is to remove the ***existing ability*** of persons to make disclosures to IGIS officials under paragraph 64(1)(a) of intercept information that is currently obtained by ASIO under a TI warrant issued under the *TIA Act*. The proposed amendment of section 64 to exclude 'ASIO computer access intercept information' without including IGIS in new section 63AC would also have the effect of removing the lawful authority of IGIS officials to deal with and communicate that information to each other for the purpose of performing their oversight functions.

The basis for proposing this amendment is unclear. All that would change as a result of the proposed amendments to the *ASIO Act* in Schedule 2 to the Bill is that some of the information that is currently disclosed to, and by, IGIS officials under paragraph 64(1)(a) would be obtained by ASIO under a different type of warrant (namely, a computer access warrant under the *ASIO Act* rather than a TI warrant under the *TIA Act*).

---

136 Schedule 2, item 124 (new s 63AC). See also item 120 (amendment to s 5(1) to insert a definition of 'ASIO computer access information' and 'ASIO computer access warrant').

137 Schedule 2, item 125,

138 Schedule 2, item 124.

139 New paragraphs 63AC(2)(d)-(i).

140 The Explanatory Memorandum states, at p. 122 at paragraph [687], that the amendment to section 64 is ***intended*** to prohibit the communication of, or other dealings with, ASIO computer access intercept information 'even if in connection with … the performance of the IGIS of his or her functions'. It may be that the absence of a provision in new section 63AC enabling disclosures to, and by, IGIS officials is an unintended oversight in the drafting of that section. However, if there is an intention to prohibit the disclosure of 'computer access intercept information' to, and by, IGIS officials, this would severely impede IGIS's ability to conduct meaningful oversight of ASIO's actions under computer access warrants. IGIS would oppose such an attempt.

Suggestion: restore the explicit authorisation for disclosures to, and by, IGIS officials

IGIS seeks the inclusion of an exception in new section 63AC for disclosures of that information to, and by, IGIS officials for the purpose of those officials performing their functions and duties and exercising their powers as IGIS officials (and the coverage of related dealings for the aforementioned purpose).

2.4.2 The need for an exception for disclosures to and by IGIS officials

It is essential to the ability of IGIS to conduct oversight of ASIO's interception and related activities that the *TIA Act* continues to provide a clear exception for the voluntary disclosure of ***all forms*** of intercept information (however described) to, and by, IGIS officials for the purpose of those officials performing their functions or duties and exercising their powers as IGIS officials.

As the Explanatory Memorandum to the Bill notes, 'it is almost always necessary for ASIO to undertake limited interception for the purpose of executing a computer access warrant'.[141] The Human Rights Statement of Compatibility in the Explanatory Memorandum also identifies IGIS oversight of ASIO's computer access warrants as a key safeguard to ensure that the new powers authorised under those warrants are 'exercised lawfully, with propriety, and with respect for human rights'.[142]

IGIS could not effectively oversee ASIO's warrant-based computer access activities without the ability to obtain, deal with and communicate the intercept information to be covered by the new concept of 'ASIO computer access warrant information'.

Schedule 5—Other amendments to the ASIO Act

5.1 Civil immunity for giving voluntary assistance to ASIO: new s 21A(1)

Schedule 5 to the Bill proposes to insert new section 21A in the *ASIO Act.*[143] New subsection 21A(1) would confer an immunity from civil liability on persons or bodies who render voluntary assistance to ASIO in accordance with a request by the Director-General of Security, or a senior position-holder to whom the Director-General has delegated the power under new subsection 16(1A).[144]

5.1.1 Legal effect

The establishment of a model of internal authorisation for the conferral of civil immunities on persons who voluntarily assist ASIO to perform any of its functions is a significant departure from the existing process for granting statutory immunities to such persons.

Currently, only the Attorney-General may confer a civil immunity on participants in a special intelligence operation (SIO) by granting an authority for such an operation under Division 4 of Part III of the *ASIO Act*. This enlivens a statutory immunity (from both civil and criminal liability) for authorised participants who engage in authorised conduct.

141 Explanatory Memorandum, p. 15 at paragraph [51] and p. 80 at paragraph [352].

142 Explanatory Memorandum, p. 16 at paragraph [61].

143 Schedule 5, item 2.

144 Schedule 5, item 1.

The Attorney-General must specifically authorise an operation as an SIO, the relevant conduct to be undertaken in that operation, and the participants.[145] SIOs may only be authorised in relation to a sub-set of ASIO's statutory functions.[146] The issuing criteria include matters directed to an assessment of the proportionality of the relevant conduct sought to be authorised, which do not have an equivalent in new subsection 21A(1).[147]

Importantly, the SIO scheme also requires ASIO to notify the IGIS as soon as practicable when an operation is authorised, and to report periodically to the IGIS (and Attorney-General) on the conduct of those operations.[148] These requirements ensure that IGIS has visibility of the circumstances in which immunities from legal liability are conferred and applied, which facilitates oversight. The civil immunity scheme in new subsection 21A(1) does not contain equivalent requirements to give IGIS visibility of the exercise of the new power to confer immunities, which may limit the practical capacity of IGIS to perform effective oversight. [149]

5.1.2 Thresholds for conferring immunity

New paragraph 21A(1)(b) enlivens an immunity from civil liability for a person or body who provides voluntary assistance to ASIO if the Director-General (or delegate) is satisfied, on reasonable grounds, that the conduct specified in a request is likely to assist ASIO in the performance of its functions.

This threshold is broad, in that it 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 otherwise 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 under subsection 17(1)(a), or ***the performance of services for ASIO*** that in some way helps ASIO in the performance of its functions. This would seem to make it possible for assistance requests under new subsection 21A(1) to be utilised as a basis upon which persons become 'ASIO affiliates' within the meaning of that term in section 4 of the *ASIO Act*. (For example, sources and members of other Commonwealth, State and Territory authorities that are cooperating with ASIO.)[150] If ASIO were to adopt a practice of using new

145 *ASIO Act,* subsection 35D(1).

146 *ASIO Act,* subsection 35D(1)(a) ('special intelligence functions').

147 *ASIO Act,* subsection 35C(2).

148 *ASIO Act,* sections 35PA and 35Q.

149 As explained at **[5.1.8] below**, IGIS supports the inclusion of notification and reporting requirements.

150 That is, a request made under subsection 21A(1) could be taken to be an 'arrangement' between the person and ASIO for the performance of functions or services for ASIO. (IGIS also notes that there may be some uncertainty as to whether a person who is ***already*** in a contract or legally binding agreement with ASIO for the provision of assistance could be covered by a request made under subsection 21A(1) in respect of the services that are the subject of the contract or agreement. As that person would be under a legal obligation to perform the services, they might not be taken to be rendering the assistance voluntarily, or in accordance with a request. However, that would not seem to prevent a pre-existing contract from being terminated and replaced by a request made under new subsection 21A(1) and supported with a new contract or agreement in relation to the conduct covered by the request under new subsection 21A(4).)

subsection 21A(1) as the means by which persons become ASIO affiliates, the result would be that civil immunity could be conferred on a very broad class of persons.

The breadth of the civil immunity conferred under new subsection 21A(1) raises several implications for oversight by IGIS of the legality and propriety of ASIO's decision-making about making requests for assistance, particularly with respect to the assessment of proportionality (as discussed below).

Oversight of proportionality related considerations

There is no statutory requirement for the Director-General or delegate to consider, and be satisfied of, the proportionality or reasonableness of any immunity from civil liability in order to make a request under subsection 21A(1).

> Suggestion: a proportionality based condition for the making of requests
>
> As with the above comments on Schedule 1 in relation to technical assistance requests, IGIS would support the inclusion of a proportionality based assessment in the statutory conditions for making a request under new subsection 21A(1), or in the *Minister's Guidelines to ASIO*. This would provide clear standards against which IGIS could conduct oversight of ASIO's decision-making.

5.1.3 Uncertainty in the coverage of conduct causing 'pure economic loss'

The immunity from civil liability is subject to some limitations, including a limitation in new paragraph 21A(1)(e) for conduct that results in significant loss of, or serious damage to, property. However, it is not clear if the concept of 'significant loss of property' would cover, or is intended to cover, so-called 'pure economic loss' sustained by a third party, which is caused by a person's conduct in accordance with a request to assist ASIO under new subsection 21A(1). Examples of this type of loss include loss of income, and decrease in the market value of property.

If conduct causing significant 'pure economic loss' is not covered by the limitation on the civil immunity in new paragraph 21A(1)(e), third parties may be deprived of a right to a legal remedy in respect of such loss. The reasons for an absence of an equivalent protection in relation to significant economic loss as for significant loss of or damage to property are not readily apparent.

It is possible that a person who suffers such loss may complain to IGIS, if they were to become aware of the reasons for their loss of their right to a legal remedy. It is open to IGIS to recommend the payment of compensation to a person who suffers harm or sustains damage as result of the actions of an intelligence agency, and to recommend the cessation or modification of the form of assistance requested by ASIO that caused the loss.[151] However, an advisory recommendation is clearly of lesser value to an aggrieved person than a legally enforceable remedy.

151 *IGIS Act,* paragraph 22(2)(b). IGIS also notes that the task of quantifying such loss would be complex.

Suggestion: an explicit statutory exclusion

To ensure clarity in the scope of the immunity, IGIS would support consideration of an explicit exclusion of conduct causing significant economic or financial loss.

As further suggested at **[5.1.8] below**, IGIS would also support reporting and notification requirements in relation to the use of the immunity.

5.1.4 No exclusion of conduct causing physical or mental harm or injury

There is no exclusion from the civil immunity for conduct that causes physical or mental harm or injury to another person. While new paragraph 21A(1)(d) excludes conduct that would involve the commission of an offence against a Commonwealth, State or Territory law, not all conduct that causes injury or harm is an offence, particularly conduct that would constitute the tort of negligence.

As with the above comments on 'pure economic loss', this may be a source of complaints to IGIS. However, in the absence of statutory notification or reporting obligations on ASIO, it would be difficult for IGIS to consistently identify those instances in which actions done in accordance with a request under new subsection 21A(1) caused harm or injury to another person, who is deprived of a legally enforceable right to a civil remedy.

Suggestion: an explicit statutory exclusion

IGIS supports consideration of an explicit statutory exclusion of such conduct from the immunity, as well as reporting and notification requirements suggested at **[5.1.8] below**.

5.1.5 Relationship with ASIO warrants and statutory authorisations

New subsection 21A(1) does not expressly exclude conduct that would require ASIO to obtain a warrant (or another form of authorisation) to undertake itself. This raises questions about how requests made under subsection 21A(1) will interact with existing warrant or authorisation requirements. IGIS would support clarification of the intended interaction.

Relationship with ASIO warrants

As a primary purpose of ASIO's special powers warrants is to provide lawful authority for activities that would otherwise constitute an offence, the above matter is managed substantially (but not entirely) by the limitation on the civil immunity in new paragraph 21A(1)(d) for conduct that involves the commission of an offence against a Commonwealth, State or Territory law.

However, not all of the conduct for which ASIO would require a warrant to undertake itself is ***necessarily*** an offence if it is undertaken by another person. For example, it may be that the Director-General makes a request of a person (*the first mentioned person*) to access data held in a computer that the first-mentioned person lawfully uses, or to obtain physical things in a house at which the first-mentioned person lawfully resides. It may be that the relevant data or things belong to, or are jointly owned or used by, another person who is of security interest to ASIO (*the second-mentioned person*). It may be that the first-mentioned person commits no criminal offence in accessing the data or things and giving them to ASIO, even if they may have otherwise been exposed to civil liability for doing so.

If ASIO sought to obtain the relevant data directly from the computer or thing on the premises, it would require authorisation under a special powers warrant (such as a search warrant, a computer access warrant or an identified person warrant) to obtain the relevant data or thing. If the first-mentioned person was assisting ASIO in the conduct of a warrant operation that person would require authorisation under section 24 of the *ASIO Act* to exercise authority under the warrant.

Relationship with other authorisation requirements

Similarly, if ASIO sought to obtain foreign intelligence, the collection of which would not require a warrant under section 27A but would require an authorisation from the Attorney-General under section 27B, the question arises as to whether it could effectively bypass the requirements of the latter provision by requesting assistance from ***another person or body*** under new subsection 21A(1) in the form of undertaking a collection activity. The limitation in new paragraph 21A(1)(d) for conduct constituting an offence would not provide a limitation in these circumstances, because the collection activities requiring authorisation under section 27B are those that do not constitute offences.

A similar question arises in relation to the interaction of new subsection 21A(1) with the SIO scheme in Division 4 of Part III of the *ASIO Act* to the extent it involves the conferral of civil immunity in relation to particular 'special intelligence conduct' that does not involve the commission of an offence. SIOs are subject to considerably higher issuing thresholds and levels of approval than the requirements under new subsection 21A(1).

Suggestion: an express limitation on the power to make s 21A(1) requests

If there is no intention for new subsection 21A(1) to effectively bypass requirements for ASIO to obtain special powers warrants (or a Ministerial authorisation under section 27B, Division 4 of Part III or any other law requiring an authorisation to engage in conduct that is not otherwise an offence) then it would be desirable for the Bill to include a further limitation in new subsection 21A(1).

This could be to the effect that new subsection 21A(1) does not apply to requests for persons to engage in conduct for which ASIO would require a warrant (or another form of Ministerial authorisation or approval) to undertake.

5.1.6 Relationship with technical assistance requests

The request-based immunity scheme in new subsection 21A(1) of the *ASIO Act* appears capable of covering the same circumstances in which ASIO could make a technical assistance request of a communications provider under new section 317G of the *Telecommunications Act* (in Schedule 1 to the Bill). However, the latter scheme includes more conditions and limitations. These include: limitations on making oral requests;[152] a 'default' 90-day period of effect for requests if no expiry date is specified (which IGIS has suggested at [1.3.1] above be replaced with a statutory maximum);[153] and express provisions governing variation.[154]

152 New subsection 317H(2).

153 New paragraph 317HA(1)(b). See also new section 317J (request for performance in a specific period, and on specified conditions) and the discussion at [1.3.1] of this submission.

154 New section 317AJ (including limitations on oral variations corresponding to those in new s 317HA).

Suggestion: statutory clarification of interaction of s 21A(1) with technical assistance requests

In the absence of provisions in the *ASIO Act* that exclude conduct that could be the subject of a technical assistance request from the voluntary assistance scheme in new subsection 21A(1), ASIO would effectively have a choice of civil immunity schemes. IGIS would support statutory clarification of the relationship between new subsection 21A(1) and technical assistance requests.

5.1.7 Period of effect of requests

Requests made under new subsection 21A(1) and the resultant immunity from civil liability are not subject to a statutory maximum period of effect. This is in contrast to SIOs, which are limited to 12 months and can only be 'renewed' through the making of a request for a new authorisation for the relevant activities.[155] It is also in contrast to the 'default' maximum period of 90 days for technical assistance requests under new subsection 317HA of the *Telecommunications Act.* (As noted at [1.3.1] above, IGIS supports the imposition of a fixed statutory maximum period of effect for technical assistance requests, which sets the outer limit of any period of effect that may be specified by the decision maker, as well as any 'default' period that applies if no expiry date is specified.)

Suggestion: a statutory maximum period of effect

Oversight would be enhanced by the inclusion of a statutory maximum period of effect, preferably aligned with that applying to technical assistance requests in Schedule 1 to the Bill (which IGIS has suggested could be 90 days, consistent with the current 'default' maximum period of effect).[156]

The practical effect of a statutory maximum period of effect would be that the Director-General or delegate would need to undertake periodic reviews of requests to determine whether they should continue (via the making of a new request, subject to the relevant conditions being met).

Further suggestion: statutory clarification of the application of s 21A(1) to 'standing assistance'

Further, it is not clear whether a request made under new subsection 21A(1) can only cover, and therefore immunise, a ***single instance*** of the specified conduct; or whether subsection 21A(1) may also authorise the making of '***standing requests'*** that cover the repetition of the relevant conduct on multiple occasions (whether 'on-call' by ASIO, or 'at-will' by the relevant person, or a combination). Such ambiguity may make oversight more difficult.

As with the earlier comments on new Part 15 of the *Telecommunications Act* in Schedule 1 to the Bill, the making of a 'standing request' would also be relevant to an assessment of the proportionality of ASIO's decision to make a request, and any terms or conditions specified in that request.

155 *ASIO Act,* paragraph 35D(1)(d).

156 *Telecommunications Act,* new paragraph 317HA(1)(b). See also: [1.3.1] above.

5.1.8 Procedural provisions

A number of procedural aspects of the power in new subsection 21A(1) may add complexity to oversight by IGIS. These matters concern: the making of oral requests; the content of requests; the legal basis for the variation and revocation of requests; and limitations in the extent to which IGIS may have visibility of the circumstances in which new subsection 21A(1) is applied and the immunity is enlivened.

Oral requests

New subsection 21A(2) provides that requests under new subsection 21A(1) may be made orally or in writing. There are no statutory limitations on the circumstances in which oral requests may be made, such as a reasonable belief that it would be impracticable to make the request in writing because of circumstances of urgency. This is in contrast with the proposed requirements applying to technical assistance requests given by in new subsection 317H(2) of the *Telecommunications Act*, which limit oral requests to circumstances in which there is an imminent risk of serious harm to a person or a substantial risk of property damage, and it is not practicable to make a written request.

While there is a requirement in new subsection 21A(3) for the Director-General or delegate to make a written record of an oral request within 48 hours of the oral request, there is no requirement for a copy of that record to be given to the person whose assistance has been requested orally. This is also in contrast with the requirements for technical assistance requests and notices given by ASIO under new subsections 317H(4) and 317M(4) of the *Telecommunications Act*, which requires a copy of the written record to be provided as soon as practicable. This may leave doubt for the person as to the limits of their civil immunity, especially if the terms of an oral request for assistance are complex.

Suggestion: statutory conditions for the making of oral requests

As a matter of propriety, IGIS would expect that requests are generally made in writing, and that also copies of written records made of any oral requests are provided as soon as practicable to the persons to whom requests are made.

However, the inclusion of these matters as statutory requirements (consistent with the requirements applying to technical assistance requests) would assist in the oversight of actions taken under new subsection 21A(1).

Content of requests

New subsection 21A(1) is not subject to an equivalent requirement to that in new subsection 317HAA(1) of the *Telecommunications Act*, which will require the Director-General to inform a designated communications provider that compliance with a technical assistance request is voluntary.

Suggestion: statutory requirement to advise a person that compliance is voluntary

The inclusion of an equivalent requirement in new subsection 21A(1) of the *ASIO Act* would be beneficial in ensuring that persons and bodies subject to such requests are clearly informed of their legal position. IGIS would oversee ASIO's compliance with that legal requirement.

Variation and revocation of requests

New section 21A does not make provision for the variation or revocation of requests for assistance, in contrast to the detailed requirements applying to technical assistance requests and notices in new Part 15 of the *Telecommunications Act* in Schedule 1 to the Bill.

This may reflect an intention to rely on subsection 33(3) of the *Acts Interpretation Act,* which provides that a power to make an instrument includes the power to vary or revoke the instrument (in the like manner and subject to like conditions, if any, for the making of the instrument). However, while it might possibly be arguable that a written request made under subsection 21A(1) could be an 'an instrument of an administrative character' for the purpose of subsection 33(3) of the *Acts Interpretation Act,* a written record of an oral request may not be.[157]

Suggestion: clarification of existence, source and scope of variation power

IGIS would be assisted by clarification of the intended source of a power to vary or revoke subsection 21A(1) requests.

Further, if new subsection 21A(1) is amended to include an explicit power of variation as well as a maximum period of effect (as suggested above) then IGIS would support an express limitation on the power to vary a request by extending its period of effect. This limitation would prohibit a request from being varied to extend or further extend the cumulative period of effect beyond the statutory maximum.

Reporting and notification requirements

The discretion to confer an immunity from legal liability is a significant power, having particular regard to the potential impacts of that immunity on third parties, who may be deprived of legal remedies for major loss, damage, injury or other harm. The conferral of such a power on members of an intelligence agency, rather than a Minister, is a significant devolution of this power.

Independent oversight by IGIS of the exercise of powers under new subsection 21A(1) would be significantly assisted by a requirement for ASIO to notify IGIS when the power is exercised, and to report periodically to IGIS on the use of that provision.

IGIS considers that the existing notification and reporting requirements in sections 35PA and 35Q of the *ASIO Act* for special intelligence operations are equally important for the oversight of acts that enliven the immunity for civil liability under that scheme as for acts that enliven the immunity for criminal liability. Accordingly, and in view of the proposed devolution of power to intelligence officials, IGIS would support equivalent types of notification and reporting requirements in relation to new subsection 21A(1).

Suggestion: statutory reporting and notification requirements to IGIS

Periodic reporting requirements could also be extended to the ASIO Minister and Attorney-General, and would usefully require the following information to be provided:

- statistical information on the use of the provision in the relevant period (perhaps annually);

157 *Laurence v Chief of Navy* (2004) 139 FCR 555 at 558 (Wilcox J).

- the types of assistance provided under section 21A (perhaps focusing on identifying significant assistance); and
- instances that are known to ASIO (if any) in which a person engaged in conduct to assist ASIO in the performance of its functions that caused significant loss of, or serious damage to, property, or other conduct that is excluded from the immunity such as the commission of an offence (and the quantum of loss if known, or an estimated quantum).

Oversight of the actions of persons providing assistance to ASIO

If a person is requested under new subsection 21A(1) to provide assistance to ASIO that comprises the actual performance of certain of ASIO's statutory functions, then the person is likely to become an 'ASIO affiliate' within the meaning of section 4 of the *ASIO Act*. Depending on the circumstances, that person may also be taken to be a 'member' of ASIO for the purpose of the *IGIS Act*. In this event, the actions of that person in providing the assistance requested under new subsection 21A(1) would be taken to be those of ASIO, and directly subject to IGIS oversight.

This would require more complex oversight arrangements in relation to the person's actions in providing the relevant assistance, as well as in relation to any 'secondary use' that may be made of the person's status as an 'ASIO affiliate' while they are rending assistance to ASIO. (Namely, their potential authorisation to exercise certain powers under the *ASIO Act* or other legislation including the *TIA Act.*) It may be appropriate that such persons are informed by ASIO of their status as an 'ASIO affiliate' as well as their obligations to cooperate with IGIS.

5.2 The compulsory provision of assistance to ASIO: new section 34AAA

New section 34AAA of the *ASIO Act* would confer a power on the Attorney-General to compel a person to provide information or assistance to ASIO that is 'reasonable and necessary' to enable ASIO to access, copy or convert data held in, or accessible from, certain computers or data storage devices. Namely, computers or data storage devices that:

- have been, or will be, accessed under various special powers warrants including computer access, search and surveillance warrants; or
- have been found and seized during the search of a person who is detained under a questioning warrant or a questioning and detention warrant.[158]

The requirements for the making of orders under new section 34AAA are modelled broadly on those applying to the making of orders to assist law enforcement agencies under existing section 3LA of the *Crimes Act 1914* in connection with search warrants issued under that Act. Some modifications are applied to reflect ASIO's specific functions. These include the conferral of the power to make orders upon the Attorney-General rather than a judicial officer; and differences in the purposes for which, and persons in relation to whom, orders may be made.

Given the coercive nature of orders made under new section 34AAA, IGIS is likely to pay close attention to ASIO's actions in requesting and executing those orders. There are some features of the proposed scheme (outlined below) that will make oversight difficult, and could be addressed with some targeted amendments.

158 New subsection 34AAA(1), Schedule 5, item 3.

5.2.1 Persons in relation to whom orders may be made

New paragraph 34AAA(2)(c) authorises the making of an order in relation to a specified person who:

- has some kind of link with the computer or device, as set out in new subparagraphs 34AAA(2)(c)(ii)-(vi); or
- is reasonably suspected of being involved in activities that are prejudicial to security, as set out in new subparagraph 34AAA(2)(c)(i).

Coverage of legal persons

It is unclear whether there is an intention for the definition of a 'person' in section 2C of the *Acts Interpretation Act* to apply to the 'specified persons' in new paragraph 34AAA(2)(c) and thereby cover legal persons (particularly bodies corporate) in addition to natural persons, especially with respect to the specified persons in subparagraph 34AAA(2)(c)(i). That is:

- Is it intended that an individual officer of a body corporate (or possibly an official of a body politic) could be the subject of an order under new section 34AAA, on the basis that the body corporate or body politic is reasonably suspected of being involved in prejudicial activities?
- If so, must the order identify a ***particular member*** of the body corporate (or body politic) to render the specified assistance?
- If so, could that individual be ***any member*** of the body corporate (or body politic), even if the named individual personally had no involvement in the prejudicial activity?

Suggestion: clarification of the intended application to legal persons

Clarification of the intended application, desirably in the provisions of the Bill, would remove potential ambiguity and assist with the oversight of ASIO's requests for orders and their execution.

Persons 'involved in' activities that are prejudicial to security

IGIS considers that the threshold in new subparagraph 34AAA(2)(c)(i) that a person is reasonably suspected of being ***'involved in'*** activities that are prejudicial to security is quite low, since there is no requirement for the person to be ***knowingly or intentionally*** involved in those activities. This raises the possibility that a person might be taken to be 'involved in' prejudicial activities because:

- the person is a conduit through which another person is acting, and their involvement may be unintentional and potentially unknown to them; or
- the person may provide products or services to another person that enable the other person to engage in prejudicial activities. The first-mentioned person may have no knowledge of the use to which their products or services are put by the second-mentioned person.

Further, new subparagraph 34AAA(2)(c)(i) does not require there to be any nexus between the prejudicial activities (or suspected prejudicial activities) in which the specified person is involved, and the security matter in respect of which the relevant warrant is issued.

This would appear to make it possible for an order to be sought and issued in relation to a person who is suspected to be involved in prejudicial activities (including unknowingly) that are ***wholly unrelated*** to the particular warrant operation, but that person is believed to possess technical

expertise in computer access and network exploitation that could be utilised to access data held in, or accessible from, a computer or data storage device that is the subject of the warrant. (In contrast, the corresponding provision in existing subparagraph 3LA(2)(b)(i) of the *Crimes Act* for law enforcement orders requires the issuing magistrate to be satisfied that the person specified in the order is 'reasonably suspected of having committed the offence stated in the relevant warrant'.)

Suggestion: clarification of intended application

This broader application of new section 34AAA of the *ASIO Act* may be unintended, noting that the justification given in the Explanatory Memorandum refers to the use of orders to compel ***'a target or the target's associate'*** to render assistance such as the provision of 'a password, pin code, sequence or fingerprint necessary to unlock a phone' (emphasis added).[159]

If a narrower application is intended, it may be desirable for new subparagraph 34AAA(2)(c)(i) to be clearly limited to persons who are involved in prejudicial activities that relate to the ***same*** security matter in respect of which the warrant mentioned in new subsection 34AAA(1) is issued.

Oversight implications if a broader application is intended

However, if a broader application is intended, IGIS is likely to scrutinise closely the basis upon which ASIO has identified (and explained in its request to the Attorney-General) that the specified person possesses the relevant knowledge under new paragraph 34AAA(2)(d); and the proportionality of a request for an authorisation to exercise coercive powers against that person, in line with paragraph 10.4(a) of the current *ASIO Guidelines.* (In considering matters of proportionality, IGIS will take into account the basis upon which the person is said to be 'involved in' prejudicial activities, and whether those prejudicial activities are the same as the security matter in the relevant warrant.)

5.2.2 Assistance that may be compelled under an order

New subsection 34AAA(3) contains a number of procedural requirements that apply if the relevant computer or data storage device ***is not*** on premises in relation to which a warrant is in force. These requirements include: the specification of the period of time in which the person must provide information or assistance and the place at which they must do so;[160] and any other conditions determined by the Attorney-General.[161]

It is not clear why the requirements in new subsection 34AAA(3) are limited to circumstances in which a computer or data storage device is not on warrant premises.

There may conceivably be circumstances in which a computer or data storage device physically remains on the warrant premises while the warrant is in force (and after the warrant ceases to be in force) but the conditions specified in new subsection 34AAA(3) would be equally important to provide certainty and transparency about the scope and limits of authority under the order, and a clear basis for IGIS to conduct oversight of ASIO's actions under the order.

159 Explanatory Memorandum, p. 143 at paragraph [877].

160 New paragraphs 34AAA(3)(a) and (b).

161 New paragraph 34AAA(3)(c).

For example, the requirement in new subsection 34AAA(3) for an assistance order to specify conditions would not seem to have any application if:

- ASIO accesses a computer remotely under a computer access warrant; or
- ASIO accesses premises under a computer access warrant or a search warrant, and data is copied from a computer on those premises without any removal of that computer, and an order is issued to require a person to provide assistance in making that data accessible to ASIO in an intelligible form (for example, applying decryption or removing other forms of protection); or
- an order is issued to require a person to provide information to ASIO while a warrant is in force but before it is executed, so that ASIO can use the information to access relevant data from a computer or data storage device during the warrant operation.

Suggestion: application of s 34AAA(3) requirements to all orders

Given the importance of the conditions specified in new subsection 34AAA(3) to the scope and limits of authority under an order, IGIS considers that those conditions should apply to all orders, irrespective of the physical location of a computer that is accessed under the related warrant.

5.2.3 Requirements relating to form, record-keeping, discontinuance and destruction

Orders made under new section 34AAA are not subject to equivalent requirements to those which apply to the underlying warrant in sections 30, 31 and 32 of the *ASIO Act.* The application of equivalent statutory parameters to new section 34AAA would assist oversight, since these orders operate in combination with special powers warrants. Specifically, existing sections 30, 31 and 32 impose requirements in relation to the matters outlined below.

The form in which requests are made

Existing subsection 32(1) imposes an obligation on the Director-General in the event a warrant is requested orally. Such a request must be followed with a written request. In contrast, new section 34AAA is silent about the form which orders or requests for orders must be made (for example, in writing or orally in defined circumstances).

Suggestion: an equivalent to subsection 32(1)

In the experience of IGIS, statutory form requirements are a valuable means of promoting consistent record-keeping practices. IGIS therefore supports an equivalent requirement to that in s 32(1).

Record-keeping requirements

Existing subsection 32(4) requires the Director-General to keep a record of all warrants issued and revoked by the Attorney-General, and all requests for warrants.

Suggestion: an equivalent requirement to s 32(4)

New section 34AAA does not prescribe any record-keeping requirements, which may make it difficult for IGIS to correlate section 34AAA orders with the underlying warrant. IGIS would be assisted by an equivalent requirement.

Obligation to discontinue action before expiration of warrant and notify Attorney-General

Existing section 30 imposes obligations on the Director-General if he or she becomes satisfied that the grounds on which a warrant was issued cease to exist while the warrant is in force. The Director-General must, as soon as practicable, notify the Attorney-General and take such steps as are necessary to ensure that action taken under the warrant is discontinued.

Suggestion: an equivalent requirement to section 30

New section 34AAA contains no equivalent requirement if the Director-General becomes satisfied that the grounds for issuing an order cease to exist during its period of effect. Consideration might also be given to extending the requirement applying to warrants under existing section 30 to related section 34AAA orders.

Secondary use and destruction of certain records of information obtained under a warrant

Existing section 31 requires the Director-General to cause the destruction of records or copies of information obtained under a warrant, if satisfied that the record or copy is not required for the performance of functions or the exercise of powers under the *ASIO Act*.

Information obtained under a section 34AAA order is not obtained under a special powers warrant, but rather an ancillary order to such a warrant. Consequently, such information is not subject to the destruction obligation in existing section 31, nor any specific limitations on its secondary use. Significantly, section 34AAA orders could involve the collection of sensitive information, including personal information. For example, the Explanatory Memorandum expressly contemplates that this could include biometric information, such as a person's fingerprints, where necessary to gain access to a computer through a biometric identification system.[162]

Suggestion: consideration of an equivalent requirement to section 31

IGIS would support consideration of statutory requirements, and supporting guidance in the *Minister's Guidelines to ASIO*, in relation to the retention, destruction, handling and secondary use of information obtained under a section 34AAA order, particularly any biometric information.

162 Explanatory Memorandum, p. 143 at paragraph [877].

5.2.4 Notification and service of orders

New section 34AAA does not contain a requirement for an order to be served on the specified person. Nor does it prescribe the date of service as the earliest commencement date for any 'compliance period' within which a person may be required to provide information or assistance under an order. This contrasts with the provisions of new Part 15 of the *Telecommunications Act* governing the duration and compliance period in relation to technical assistance requests, and technical assistance and capability notices.[163]

Suggestion: statutory notification or service requirements

As a matter of propriety, IGIS would expect that orders are served on the specified person; that ASIO's requests for orders suggest a condition that any 'compliance period' commences from either the date of service or a later date as specified; and that the duration of any suggested compliance period is reasonable in all of the circumstances. However, given the coercive nature of orders under section 34AAA it may be preferable for these matters to be prescribed as legislative requirements.

5.2.5 Possibility that a person attending under an order may be taken to be in detention

There is a question as to whether a person who is required to attend a place to provide information or assistance to ASIO under a section 34AAA order may be subject to a form of detention; and if so, whether there are adequate safeguards in new section 34AAA.

These questions may arise if the person is led to believe that they are not free to leave the place of attendance if they sought to do so. For example, due to the physical obstruction of exit points; or an indication to the person that they would, or may, be arrested on suspicion of the offence in new subsection 34AAA(4) if they attempted to leave without attempting to provide the assistance or information.[164] The risk that a person may be taken to be in detention by attending a place in compliance with an order may also arise due to the absence of statutory maximum time periods for attendance.[165]

163 New sections 317HA and 317J (technical assistance requests) ;317MA and 317N (technical assistance notices); and 317TA and 317U (technical capability notices). See also, new s 317ZL (service of technical assistance and capability notices).

164 See, for example: United Nations Human Rights Committee, *General Comment No. 35 Article 9 (Liberty and Security of the Person)*, 112th Sess, UN Doc CCPR/C/GC/35 (2014) at [5]-[6].

165 If a person is taken to be in detention, or otherwise deprived of their liberty while in attendance under a notice, there is also a question as to whether the deprivation of liberty is arbitrary. In this regard, IGIS notes that some aspects of proposed section 34AAA may create a risk that orders may be issued or executed in a way that a person is arbitrarily detained or deprived of liberty. In particular, orders can be issued in relation to persons who may not have had any involvement, or knowing involvement, in activities prejudicial to security; and in relation to persons who have been involved in prejudicial activities that are wholly unconnected with the relevant warrant, but are thought to possess relevant technical expertise.

Suggestion: consideration of whether further statutory safeguards are needed

IGIS will pay close attention to the proposed terms of an order sought by ASIO, in assessing whether the information and assistance sought is 'reasonable and necessary' as required by new subsection 34AAA(1). However, consideration might be given to whether the *ASIO Act* or the *Minister's Guidelines* should include further safeguards, including against the risk of arbitrary deprivation of liberty in connection with section 34AAA.

IGIS notes that section 3LA of the *Crimes Act* does not make specific provision for the fact that a person who is the subject of an assistance order under that provision might be taken to be in detention. However, an important distinction is that those orders are issued by a judicial officer rather than a Minister.

5.2.6 Interaction of section 34AAA orders with other coercive powers

There is also a question of how a requirement for a person to attend a place and provide information or assistance under a section 34AAA order may interact with ASIO's compulsory questioning and detention powers under Division 3 of Part III of the *ASIO Act*, or technical assistance notices issued by ASIO under the proposed amendments to the *Telecommunications Act* in Schedule 1 to the Bill.

Concurrent operation of section 34AAA orders with questioning and detention warrants

New paragraph 34AAA(1)(a)(ix) enables orders to be issued to compel assistance ***or information*** in relation to accessing data held in, or accessible from, a computer or data storage device that has been seized under section 34ZB during a search of a person being detained under a questioning warrant or a questioning and detention warrant.

In particular, if a device is seized under section 34ZB, could the person then be required to comply with an order under section 34AAA while the questioning warrant or questioning and detention warrant is in force? (For instance during a break in questioning under the warrant?) If so, complex questions may arise about the interaction of the two schemes, including the legal basis for the presence and role of the IGIS while the section 34AAA order is being executed (noting that the specific provisions of Division 3 of Part III of the *ASIO Act* would not apply to new section 34AAA). Neither the Bill nor the Explanatory Memorandum address this scenario.

Suggestion: statutory clarification of the interaction of s 34AAA with questioning and detention

IGIS supports clarification of the intended operation of orders under new section 34AAA in relation to persons who are being detained under a questioning or questioning and detention order.

Potential for the exercise of multiple coercive powers against a person

Issues of potential oppression may also arise as a result of the exercise of multiple coercive powers in relation to a person to obtain the same or substantially similar information.

For example, there is the possibility that ASIO may exercise coercive powers to require a person to provide their access credentials to a computer a section 34AAA order; and subsequently under a questioning warrant, or if the person is a communications provider, under a technical assistance notice issued by ASIO. There is also the possibility that ASIO may exercise coercive powers to obtain

such information from a target who is also under investigation by law enforcement agencies, and is or was subject to coercive powers exercised by those agencies (for example, under section 3LA of the *Crimes Act*).

In examining ASIO's requests to the Attorney-General for the making of section 34AAA orders (and its requests for the issuing of questioning warrants or questioning and detention warrants, or the issuing of technical assistance notices), IGIS is likely to examine evidence of ASIO's consideration of whether the person has been subject to requests for authorisations to exercise other coercive powers in relation to the same or a substantially similar matter, and if so, the reasons for which a further request is being made.

IGIS also would also consider whether the Attorney-General has been specifically informed of the exercise, or potential exercise, of multiple coercive powers against a person in all requests for authorisations to exercise coercive powers made by ASIO.

Suggestion: statutory requirements for requests to the Attorney-General under s 34AAA

IGIS would support a statutory requirement for ASIO to include in all requests made to the Attorney-General for orders under section 34AAA information about previous orders and requests for orders in relation to a person, consistent with the requirements applying to requests for questioning warrants under existing section 34D.

5.2.7 Reporting requirements

The Bill does not impose any specific Ministerial reporting requirements on ASIO in relation to orders made under section 34AAA. The Ministerial reporting requirements under existing section 34 (special powers warrants) and 34ZH (questioning warrants and questioning and detention warrants) are expressly limited to 'action taken under the warrant' and therefore would not cover action taken under a section 34AAA order relating to a warrant.

Suggestion: statutory reporting requirements for s 34AAA (aligned with warrant reports)

A reporting requirement in relation to new section 34AAA orders could usefully be integrated with the existing warrant reporting requirements in sections 34 and 34ZH. This would help to ensure that the IGIS, the responsible Minister for the agency and the Attorney-General have a comprehensive picture of how the relevant warrant and any related section 34AAA orders have ***collectively*** assisted ASIO in the performance of its functions.

5.2.8 Secrecy obligations

Orders made under new section 34AAA do not appear to be subject to any specific secrecy offences for disclosures of their contents or existence by persons who are subject to them. This is in contrast with the specific secrecy offences for persons who are the subject of questioning warrants or questioning and detention warrants under existing section 34ZS of the *ASIO Act*, and the new secrecy offences in Schedule 1 to the Bill for persons who disclose information about requests and notices issued under new Part 15 of the *Telecommunications Act.*

IGIS questions whether this may reflect a view that a person who is the subject of a section 34AAA order is liable to the secrecy offences in subsection 18(2) and sections 18A and 18B of the *ASIO Act*. This would only be possible if the person was taken to be an 'ASIO affiliate' or an 'entrusted person'

who has entered into an 'arrangement' with ASIO ***other than*** as an ASIO affiliate, within the meaning of those terms in section 4 of the *ASIO Act.* Alternatively, it is possible that there is an intention to place sole reliance on the general secrecy offences in new Division 122 of the *Criminal Code* for disclosures of 'inherently harmful information'. In either case, to the extent that these existing offences would cover disclosures of information about a section 34AAA order, they contain sufficient provision for the disclosure of that information to, and by, IGIS officials (in addition to the immunities conferred under subsection 18(9) and section 34B of the *IGIS Act* for compulsory and voluntary disclosures of information to IGIS officials).

However, as noted in the earlier comments on Schedule 1 to the Bill, there may be doubt that a person who is the subject of a section 34AAA order could be an 'ASIO affiliate' or otherwise an 'entrusted person' by reason of that order. It is arguable that these concepts apply only to persons who ***voluntarily*** enter into some form of relationship with ASIO (that is, under a contract, agreement or other arrangement) and do not extend to relationships that are created by the exercise of coercive powers.

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 Assessments (ONA).

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 Office has 28 staff at 12 October 2018.

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.[166] 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. IGIS staff have access to all documents of the intelligence agencies, and the IGIS is often proactively briefed about sensitive operations.

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 are being increased to allow the office to sustain a full time equivalent staff of 55 and to allow the agency to move to new premises.[167] The IGIS will also assume oversight functions in relation to the Office of National Intelligence (ONI) following passage of legislation presently before the Parliament to establish that agency as the successor to ONA.[168]

---

166 See *IGIS Act,* section 8 in relation to the general jurisdiction of the IGIS.

167 The Hon M Turnbull MP, Prime Minister and Cabinet Portfolio Budget Statements 2018-19, *Budget Related Paper No. 114*, 8 May 2018, p. 278 (an additional $52.1 m over 5 years from 2017-18).

168 Office of National Intelligence Bill 2018*;* and Office of National Intelligence (Consequential and Transitional Provisions) Bill 2018.

UNCLASSIFIED

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Supplementary submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone

Inspector-General of Intelligence and Security

23 November 2018

Introduction

On 14 November, the Committee published a supplementary submission of Department of Home Affairs (submission 18.3). That supplementary submission responds to some of the matters raised in the Inspector-General of Intelligence and Security (IGIS) submission to the inquiry (submission 52) concerning proposed amendments to the *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*) in Schedules 2 and 5 to the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill).

IGIS welcomes the Department's indication that it is considering the matters raised in the IGIS submission, and intends to engage with IGIS.[1] IGIS also welcomes the explanations given by the Department of the ways in which some of the new powers are intended to be exercised. IGIS notes that the suggestions made in our submission for some targeted amendments could help to ensure that the legislation gives clear effect to, and does not unintentionally exceed, the stated intent. This could facilitate effective compliance with, and robust oversight of, the new measures.

Key issues

IGIS makes this supplementary submission to address a number of issues raised by the Departmental submission in explaining why certain provisions are considered necessary, and why certain suggested amendments are considered unnecessary. These issues are outlined below, and concern the interpretation of existing and new provisions of the *ASIO Act*.

Computer access warrants (Schedule 2)

(1) Telecommunications interception (TI)*:* The stated case for the proposal to require all computer access warrants to authorise the use of force against persons and things for the purpose of carrying out TI appears to rely on a need to use force to enter premises for the purpose of conducting TI. The use of force to enter premises is authorised under existing provisions.

(2) Post-warrant concealment powers: The effective reduction of existing safeguards for activities carried out for the purpose of concealment (and in particular, for activities that are likely to cause material interference with the lawful use of a computer, or material loss or damage to a lawful user of a computer).

(3) Temporary removal of computers and 'other things' from warrant premises: The meaning of 'other things' that can be removed temporarily, and the duration of their removal.

Section 34AAA compulsory assistance orders (Schedule 5)

(4) Reliance on implied limitations and executive discretion as a primary source of the legal parameters on the power to compel persons to render certain assistance to ASIO.

Subsection 21A(1) civil immunities for voluntary assistance (Schedule 5)

(5) A range of issues concerning the issuing and administration of requests, including: proportionality of decisions to confer immunities; maximum duration; oral requests, variation and revocation; and interaction with ASIO warrants and technical assistance requests.

Notification and reporting requirements

(6) The importance of notification and reporting requirements to the effective oversight of extended warrant powers, powers to compel assistance, and to confer immunities from liability.

1 Department of Home Affairs, *Supplementary Submission 18.3*, p. 16 at [73], and p. 20 at [105].

1. ASIO's computer access warrants (Schedule 2)

1.1 Telecommunications interception: use of force

Issue

Schedule 2 proposes to amend the *ASIO Act* to enable computer access warrants to authorise ASIO to conduct TI for the purpose of doing any thing specified in the warrant.[2]

IGIS identified a number of potentially unintended consequences arising from this power, including that it would attract the operation of existing provisions that require all computer access warrants to authorise the reasonable and necessary use of force against persons and things for the purpose of doing the acts specified in the warrant. IGIS noted that this would be a material expansion of ASIO's existing TI powers under the *Telecommunications (Interception and Access) Act 1979* (*TIA Act*), as warrants issued under the *TIA Act* do not authorise the use of force against persons or things.[3]

Departmental submission

The Departmental submission appears to suggest that there is a need for ASIO to use force against persons and things for the purpose of conducting TI, stating that:

> *[I]t is long standing practice that entry onto premises may be necessary where it would be impractical or inappropriate to intercept communications in respect of a device otherwise than by using equipment installed on specified premises.*
>
> *This may be due to technical reasons connected with the operation of the service or the telecommunications system of which the service is part, or because the execution of the computer access warrant as a result of action taken by an officer of a carrier might jeopardise the security of the investigation. Accordingly, it is reasonable and necessary to ensure that law enforcement officers undertaking these activities can do so with appropriate authorisations around the use of force.*[4]

IGIS comment

The above explanation appears to conflate a case for using force to enter premises with a case for using further force to carry out TI at those premises once entry is gained. Existing paragraphs 25A(5A)(a), 27A(2)(a) and 27J(3)(d) of the *ASIO Act* already authorise the use of force to enter premises (provided that entry to premises is specified in the relevant warrant).

It is not apparent from the above explanation why an authorisation to use force is needed ***specifically*** for the TI component of a warrant operation (and particularly the use of force against persons) ***in addition to*** the existing authorisation of the use of force for the purpose of entering premises at which an interception activity may be carried out. IGIS oversight of ASIO's TI warrants under the *TIA Act* has not identified any cases in which ASIO has been unable to execute a TI warrant because it could not use force against a person or a thing to conduct an interception activity.

---

2 Schedule 2, items 6 and 11: new ss 25A(4)(ba) and 27E(2)(ea).

3 IGIS, *Submission 52,* pp. 42-43.

4 Department of Home Affairs, *Supplementary Submission 18.*3, p. 6 at [19].

The above explanation also refers to the reasonableness and necessity of ***law enforcement officers*** being authorised to use force against persons and things for the purpose of conducting TI. It should be noted that the power to use force under the *ASIO Act* is not limited to law enforcement officers whose assistance is made available to ASIO.

1.2 Post-warrant concealment powers

Issue

Schedule 2 proposes to amend the *ASIO Act* to extend ASIO's powers to undertake acts that are reasonably necessary to conceal actions done under a warrant. This includes a power to undertake specified intrusive activities for the purpose of concealment. The power to engage in these concealment-related activities extends beyond the duration of a warrant. It does not require the Attorney-General to specifically authorise concealment but rather applies to all warrants issued.[5]

IGIS identified that the one of the new concealment powers is not subject to equivalent limitations and prohibitions on the exercise of the same power for the purpose of accessing and manipulating data held in, or accessible from, a computer. This is the power to use a computer or a communication in transit, including adding, copying or deleting data.[6] The new concealment powers do not contain equivalent limits to those in existing subsections 25A(5), 27A(1)(a) and 27E(5) of the *ASIO Act,* which provide as follows:

- it is only lawful to do any thing that is likely to materially interfere with, interrupt or obstruct a communication in transit if it is ***necessary*** to do one or more of the things authorised in the warrant; and
- it is ***not lawful*** to do any thing that is likely to cause material loss or damage to other persons lawfully using a computer.

Departmental submission

The Departmental submission indicates that the non-application of the existing limitations and prohibitions in subsection 25A(5) (and equivalent provisions ins sections 27A and 27E) to concealment activities under the new powers is considered 'necessary to maintain operational integrity through the manipulation of data'. The submission also indicates that the non-application of the existing safeguards to the new concealment powers is considered to be reasonable and proportionate because 'the purposes for which they are abrogated are very limited'.[7]

5 Schedule 2, items 7, 8 and 12: new ss 25A(8), 27A(3C) and 27E(6).

6 IGIS, *Submission 52,* pp. 48-49.

7 Department of Home Affairs, *Supplementary Submission 18.3,* p. 11 at [50].

IGIS comments

Removal of safeguards from existing concealment powers

As noted in the IGIS submission, existing paragraphs 25A(4)(c), 27A(1)(a) and 27E(2)(f) of the *ASIO Act* currently enable the Attorney-General to authorise ASIO to undertake certain concealment activities while a computer access warrant is in force. Leaving aside the uncertainty about how the existing concealment provisions will interact with the new concealment powers while a warrant is in force,[8] it is notable that the existing concealment provisions ***are subject to*** the limitations and prohibitions on actions likely to cause material interference, or material loss or damage, in existing subsections 25A(5) and 27E(5) and existing paragraph 27A(1)(a), which applies subsection 25A(5).

It is unclear from the above justification why an effective reduction of existing safeguards is needed, especially with respect to the removal of the prohibition on concealment activities that are likely to cause material loss or damage to lawful computer users. In conducting oversight of ASIO's computer access warrants, IGIS has not identified circumstances in which ASIO has been unable to carry out a concealment activity in reliance on existing paragraphs 25A(4)(c), 27A(1)(a) or 27E(2)(f) due to the limitations and prohibitions in subsections 25A(5), 27A(1) and 27E(5) on acts that are likely to cause material interference, loss or damage to lawful computer users.

Compliance and oversight implications

The non-application of existing safeguards to the new concealment powers may also make compliance and oversight difficult. The same or substantially similar activities would be governed by different legal standards based on the specific purpose for which those activities were conducted.

For example, if ASIO sought to use a computer or a communication in transit to gain access to relevant data, it would be subject to the existing limitation on causing material interference and the prohibition on causing material loss or damage. However, if ASIO sought to use a computer or a communication in transit for the purpose of concealing its activities under a warrant (or further concealing its concealment-related actions) then no specific limitations and prohibitions would apply. This may create confusion and compliance risk among officers executing warrants, particularly if these persons need to perform 'access' and 'concealment' related activities in close proximity.

Breadth and duration of new concealment powers

Given the considerable duration and breadth of the new concealment powers, IGIS is doubtful that concealment can be characterised as a 'very limited' purpose for which acts likely to cause material interference, loss or damage can be authorised without the existing, specific limitations.

Concealment activities could be carried out for a prolonged period of time, covering the duration of the warrant (up to six months) and 28 days after its expiry, or at the earliest time thereafter that is reasonably practicable. As the concealment powers extend to the subsequent concealment of concealment-related activities, it is conceivable that post-warrant concealment activities could be carried out for an extended period of time beyond 28 days after the expiry of the warrant.

8 As noted in IGIS, *Submission 52,* p. 48.

Further, the breadth of the definition of a 'computer' in section 22 of the *ASIO Act* means that a single computer access warrant could authorise access to, and concealment activities in relation to, a large number of individual computers. (A 'computer' is defined to mean all or part of one or more computers, computer systems, computer networks, or any combination of these.)

If there is an intention to authorise ASIO to cause material interference without a specific 'necessity' threshold, and to cause material loss or damage to lawful computer users, IGIS would support an extension of the reporting requirement in section 34 to require ASIO to report on concealment activities that cause material loss or damage (in addition to the existing requirement to report on acts that cause material interference). It would also be particularly important for warrant reports to be provided separately to reports on post-warrant concealment activities.[9] This would ensure that post-warrant concealment did not delay the provision of reports on the warrant itself, including notification of material loss or damage caused by concealment activities during the warrant period.

1.3 Temporary removal of computers and 'other things' from premises

Issue

Schedule 2 proposes to enable computer access warrants to authorise the temporary removal of computers and other things from warrant premises, for the purpose of doing a thing specified in the warrant or for the purpose of concealment.[10]

The IGIS submission identified several ambiguities in the new powers and limitations in applicable reporting requirements that would make oversight difficult. This included an observation that the meaning of the 'other things' that may be removed from premises is unclear. IGIS also suggested that consideration is given to a requirement to limit the period of time for which ASIO may remove a computer or other thing from premises within the warrant period. (For example, a requirement that removal may only occur for as long as is reasonably necessary to do the particular thing under the warrant that was the purpose of the removal.)[11]

Departmental submission

The Departmental submission indicated the words 'other things' are intended to denote a category of 'things that are, in some way, needed to execute the [computer access warrant]'. It also noted that 'the Attorney-General is empowered to specify conditions relating to the return of the computers and other things' and that the power to temporarily remove a thing is limited to the duration of the warrant.[12]

9 As suggested in IGIS, *Submission 52,* p. 49.

10 Schedule 2, items 5 and 10: new ss 25A(4)(ac) and 27E(2)(da).

11 IGIS, *Submission 52,* pp.43-48, especially at pp. 44-45.

12 Department of Home Affairs, *Supplementary Submission 18.3,* p. 12 at [53].

IGIS comment

Meaning of 'other things' that may be removed from premises

Even if the words 'other thing' were given the interpretation suggested by the Department, this would not remove uncertainty identified in the IGIS submission about whether a particular thing had the requisite nexus with an activity authorised by the warrant. As warrants authorise a wide range of activities, including accessing premises, that nexus would be very broad and unlikely to provide meaningful guidance or limitation on the things that may be removed, especially in advance of their removal. There would also remain legal uncertainty about whether this construction is correct.[13]

IGIS therefore continues to support explicit statutory clarification of the 'other things' that can be removed from premises in addition to computers (for example, by creating a class of things in the nature of computer peripheral devices, which would include data storage devices and electronic equipment). Alternatively, the temporary removal power could be limited to the purpose of doing specific things under a warrant that are for the direct purpose of gaining access to relevant data held in the target computer and subsequent concealment of those activities (for example, the acts authorised by paragraphs 25A(4)(a), (ab) and (b) and equivalent provisions in sections 27A and 27E).

Duration of temporary removal

IGIS agrees with the reasoning implicit in the Departmental submission that new paragraphs 25A(4)(ac) and 27E(2)(da) confer a 'compound' power to remove ***and*** then return computers and other things. That is, the power to remove a computer or other thing would be is conditional on its subsequent return, and both actions must be done during the warrant period.

The comments raised in IGIS's submission are directed to a different issue. A maximum removal period equivalent to the total duration of the warrant may be a protracted length of time (up to six months). The removal period for post-warrant concealment activities may be open-ended (28 days after expiry of the warrant, or the earliest practicable time thereafter). To ensure the proportionate exercise of the removal power, IGIS continues to support further statutory parameters on the duration of removal ***within*** the warrant period or post-warrant concealment period.

In particular, new paragraphs 25A(4)(ac) and 27E(2)(da) could be made subject to similar conditions to those in existing subsections 25(4C) and 27D(5) in relation to the removal of things from premises under an ASIO search warrant. This would mean that a computer or other thing may only be removed for as long as is reasonably practicable to do the act or thing that is the purpose of removal. Or, if the return of the computer or other thing would be prejudicial to security after this time, it may only be retained until its return would no longer be prejudicial. In addition to providing clarity, such conditions may help to ensure that the limits of the new temporary removal powers are not unavoidably breached if a computer or other thing could not be returned while a warrant is in force because this would cause prejudice to security.

---

13 In particular, the words 'other thing' could be construed by reference to the preceding word 'computer', or by reference to the purpose of the warrant to authorise access to relevant data held in the target computer. On this interpretation, the 'other thing' would need to have a direct connection with ***a computer on the premises***, or the ***target computer specified in the warrant***. This is ***narrower*** than a nexus with the general purpose of 'executing the warrant' by doing one of the authorised things. Significant ambiguity may therefore remain, which may complicate compliance and oversight.

2. Compulsory assistance orders to ASIO (s 34AAA, Schedule 5)

Issue

New section 34AAA proposes to confer a new coercive power on ASIO via a scheme of 'assistance orders' under which the Attorney-General may, at ASIO's request, issue an order requiring certain persons to assist ASIO in accessing data held in, or accessible from, a computer or data storage device that is accessed or seized by ASIO under warrant.[14] The IGIS submission identified a number of ambiguities and apparent limitations in safeguards to the issuing and execution of these orders.[15]

Departmental submission

The Departmental submission commented on some of the matters raised in the IGIS submission, noting that it was continuing to consider the matters raised by IGIS.[16] Its initial comments indicated:

- there is an intention for assistance orders to be available in relation to persons who are unknowingly or unintentionally involved in activities that are prejudicial to security;[17]
- there is no intention for assistance orders to authorise the deprivation of liberty or inhumane treatment of persons who are providing assistance under compulsion;[18]
- the requirements in new subsection 34AAA(3) for assistance orders to specify certain conditions (the place a person must attend including the compliance period) are intended to be ***additional safeguards*** to be applied only if a computer is not on warrant premises, rather than essential matters to be specified in all orders. This seems to be based on an intention that if a computer is ***not*** removed from premises, 'it is implicit that the person will provide assistance at the time of the warrants executions and in a manner consistent with the issued warrant';[19]
- the requirements for a person to be served with an assistance order, and for any compliance period to commence no sooner than the time of service, are considered to be 'implicitly provided for' in elements of the offence for non-compliance in subsection 34AAA(4);[20] and
- the Department intends to work with the IGIS to determine if further amendments are needed to enable effective oversight of the potential for multiple coercive powers, including assistance orders, to be exercised against a person in relation to the same or substantially similar matters.[21]

14 Schedule 5, item 3.

15 IGIS, *Submission 52,* pp. 59-67.

16 Department of Home Affairs, *Supplementary Submission 18.3,* p. 16 at [73].

17 Ibid, p. 7 at [26] and p. 19 at [99]-[100].

18 Ibid, p. 16 at [75]-[76].

19 Ibid, p. 19 at [101]-[102].

20 Ibid, p. 20 at [103].

21 Ibid, p. 20 at [104]-[105].

IGIS comment

Persons who are unknowingly or unintentionally involved in prejudicial activities

IGIS is assisted by the Department's confirmation that assistance orders are intended to be available in relation to persons who are unknowingly or unintentionally involved in activities that are prejudicial to security. This may mean that orders could be issued in relation to a very broad range of persons. (For example, telecommunications carriers and carriage service providers and others in the communications supply chain whose provision of services, facilities or equipment may unknowingly enable users to engage in communications to advance prejudicial activities.)

As noted in the IGIS submission, the basis upon which a person is said to be 'involved in' prejudicial activities will be a factor that IGIS considers in assessing the proportionality of ASIO's requests to the Attorney-General for the issuing of assistance orders, in line with the requirements of paragraph 10.4 of the current *ASIO Guidelines.* The nature and degree of a person's involvement in prejudicial activities will also be material to an assessment of the propriety of ASIO's actions in considering whether to request the issuing of an order subject to conditions, and if so, the substance of those conditions. Consequently, IGIS continues to support the updating of the *ASIO Guidelines* to provide specific guidance on proportionality and other matters with respect to assistance orders.

Safeguards against arbitrary deprivation of liberty, including access to the IGIS

IGIS welcomes the statement of policy intention that assistance orders should not authorise the detention or arbitrary deprivation of liberty of the persons who are compelled to attend a specified place to provide information or assistance to ASIO. IGIS suggests that the Committee considers whether the Bill contains adequate safeguards to ensure that the power cannot be exercised in a manner contrary to the stated intent.

The Departmental submission also appears to indicate that statutory safeguards relating specifically to access to the IGIS are considered to be unnecessary, such as requirements for ASIO to inform a person of their right to complain to IGIS; and to ensure that the person has access to facilities to make such a complaint while attending a place under compulsion. This was said to be because 'information pertaining to lodging complaints against ASIO with the IGIS is freely available and the IGIS is empowered to inspect requests to the Attorney-General for assistance orders'.[22]

IGIS cautions against assuming that all individuals who come into contact with ASIO under an assistance order will be independently aware of the role of the IGIS and their right to make a complaint. It would also be unsound to assume that persons who attend a place under compulsion will necessarily have access to facilities to contact IGIS to make a complaint about their treatment while they are in attendance.

Further, IGIS's inspection function alone may not be sufficient to ***prevent*** the risk that an order may be executed against a person in a manner results in an arbitrary deprivation of liberty. This is because IGIS inspections are conducted on a retrospective basis (after a warrant, or in this case an assistance order, is issued and executed).

22 Department of Home Affairs, *Supplementary Submission 18.3,* p. 16 at [76].

Consequently, it would also be necessary for there to be a mechanism to ensure that persons who are subject to assistance orders are informed of their right to complain to IGIS while they are attending a place under an order, and to ensure that they have facilities to do so at this time.

Conditions that must be specified in assistance orders

IGIS remains of the view that the requirements in subsection 34AAA(3) are necessary components of ***any*** coercive assistance order that operates in connection with an ASIO warrant; and not merely additional safeguards that are needed only if ASIO has removed a computer from premises.

The Departmental submission suggests that, where a computer is not removed from premises, the essential conditions of the kind listed in subsection 34AAA(3) would in some way be 'implicit' in assistance orders, arising from the terms of the underlying warrant. IGIS considers that reliance on this assumption would raise significant legality and propriety risks.

It would be preferable for section 34AAA to include a statutory requirement for all assistance orders to explicitly state all of the relevant details about a person's compliance obligations, such as the place and time at which the person must attend to give assistance; or other particulars about how the assistance is to be provided, for example, a compliance period for the provision of information. This would ensure that a person who is subject to an order is made aware of his or her obligations and rights; and that these details are placed before the Attorney-General in all requests for orders.

Service requirements

IGIS is concerned that reliance on 'implied' requirements for the service of orders does not provide certainty about the content of a person's compliance obligations, or ASIO's obligations in relation to requesting and executing orders. IGIS continues to support statutory requirements.

Multiple coercive powers

IGIS would welcome consultation by the Department on this matter. As a starting point, a provision in the nature of section 34D of the *ASIO Act* (requirements for requests for questioning warrants) would provide a useful model for a statutory requirement for ASIO to inform the Attorney-General of previous assistance orders issued or requested in relation to a person, and other coercive powers.

3. Civil immunity for voluntary assistance to ASIO (s 21A, Schedule 2)

Issue

New subsection 21A(1) proposes to authorise the Director-General of Security, or a delegate, to confer civil immunities on persons who voluntarily assist ASIO in the performance of its functions, in accordance with a request made by the Director-General or delegate.[23] The IGIS submission identified a number of apparent gaps and limitations in safeguards in the scope of, and issuing thresholds for, the power to confer civil immunities; and in procedural provisions.[24]

23 Schedule 5, item 2 (and power of delegation in item 1).

24 IGIS, *Submission 52,* pp, 51-59.

Departmental submission

The Departmental submission commented on some issues raised in the IGIS submission, including:

- Section 21A requests are not intended to be used interchangeably with technical assistance requests (TARs) under the *Telecommunications Act* (Schedule 1), although there is no statutory prohibition on the use of section 21A requests in a manner that is contrary to that intent;[25]
- Section 21A requests are not intended to circumvent ASIO's existing warrant requirements;[26]
- The civil immunity is not subject to a specific exclusion of conduct causing serious harm or injury to a person. The Department stated that it considers the existing limitations (directed to loss of or damage to property, and conduct constituting an offence) 'are sufficiently broad to capture instances of meaningful harm to other persons'; as well as the voluntary nature of requests, and the seniority of the Director-General as the person exercising the power to confer immunity;[27]
- It is not considered necessary for requests (and therefore the civil immunity) to be subject to a maximum duration for various reasons relating to: the voluntary nature of requests; the intended exercise of the new power (including in connection with a warrant); and the potential for associated contracts, agreements or other arrangements to specify a compliance period;[28]
- It is not considered necessary to limit the circumstances in which requests can be made orally (namely, if circumstances of urgency would prevent them from being made in writing) because 'the Department is comfortable with the current approach as it provides flexibility for ASIO to issue an assistance request in a format that is most appropriate for the operational circumstances';[29] and
- It is intended that the power to issue a request also contains implied powers to vary or revoke that request (separately to the power in subsection 33(3) of the *Acts Interpretation Act* in relation to the power to revoke or vary decisions made by instrument).[30]

IGIS comments

Relationship of section 21A requests with TARs and special powers warrants

IGIS welcomes the acknowledgement that section 21A requests are not intended to be used interchangeably with TARs, or to circumvent requirements for ASIO to obtain a warrant.

This intent is not implemented by the provisions of section 21A. An express provision would ensure that section 21A requests can ***only*** be utilised in accordance with the policy intent, and that the intended use of section 21A is clearly communicated to all persons who may exercise powers under the provision, or who are affected by the exercise of those powers. It could take the form of a

25 Department of Home Affairs, *Supplementary Submission 18.3,* pp. 16-19 at [78]-[96].

26 Ibid, p. 17 at [85].

27 Ibid, p. 17 at [81]-[84].

28 Ibid, p. 17 at [87]-[88].

29 Ibid, p. 18 at [94].

30 Ibid, p. 19 at [95]-[96].

'relationship with other laws' provision to the effect that a section 21A request cannot be issued in circumstances in which a TAR could be issued; or if ASIO would require a warrant or an authorisation to undertake the relevant activity.

Conduct causing serious personal harm or injury

IGIS remains of the view that a statutory exclusion of conduct causing serious personal harm or injury is needed to provide a clear safeguard to the proportionate exercise of the power to confer civil immunities, which facilitates both compliance and oversight. The provisions of subsection 21A(1) do not support a conclusion that the legislative framework governing the conferral of civil immunities excludes all 'instances of meaningful harm to other persons'. Conduct constituting the tort of negligence would not be excluded from the immunity, since the civil standard for negligence falls short of criminal thresholds, but can result in loss of life and serious personal injury or harm.

The fact that compliance with a request made under subsection 21A(1) is voluntary does not ameliorate the risk that the provision will confer a power to grant immunities for conduct that causes serious harm or injury to third persons. The discretion of the person whose assistance is requested is not a substitute for safeguards to ensure that ASIO's decisions to confer immunities are proportionate; and that ASIO has means to ensure that acts done in reliance on the immunities it has conferred are, and remain, proportionate.

IGIS cautions against relying primarily on the level of seniority of a decision maker in substitution of clear statutory parameters on the exercise of discretion by that person to ensure the proportionality of the decision. This is particularly important where powers conferred on an agency head are delegable to a large number of persons, as is the case for the power to confer immunities under new subsection 21A(1).

Maximum duration

IGIS continues to support a statutory maximum period of effect for the immunities conferred under new subsection 21A(1). The Departmental submission appears to indicate that civil immunities are not intended to operate indefinitely (and may be linked, for example, to the duration of an individual warrant operation; or the terms of a contract made under subsection 21A(4) in relation to conduct engaged in under the request). Attempts to imply a period of effect into a request from the terms of a separate legal instrument such as a warrant or a contract would introduce significant complexity and uncertainty. A statutory maximum period of effect would also provide a mechanism for the periodic re-assessment of whether an immunity remains necessary and proportionate.

Oral requests

IGIS continues to support a default requirement that requests are to be made in writing, unless it would be impracticable for a request to be made in writing due to circumstances of urgency. It is common that powers which authorise activities that would impact significantly on the legal rights of other persons are required to be exercised in writing, unless the decision-maker is satisfied that there would be some kind of operational detriment in giving written authority. It is unclear from the explanation provided in the Departmental submission why a general requirement to make a request in writing, subject to an exception to enable the making of an oral requests in urgent circumstances, would unacceptably limit operational flexibility.

Reliance on implied powers of variation and revocation

There can be significant legal uncertainty about the existence, scope and limits of implied powers to vary or revoke administrative decisions. An express statutory power to vary and revoke section 21A requests (consistent with technical assistance requests in Schedule 1) would be important in providing clarity and certainty to persons who are the subject of requests, and in providing clear and transparent standards against which IGIS could conduct oversight.

4. Notification and reporting requirements (Schedules 1, 2 and 5)

Issue

The IGIS submission and the evidence of the Inspector-General at the public hearing on 16 November identified an absence of reporting and notification requirements applying to the new powers to compel assistance and to confer broad civil immunities in Schedule 1 (concerning ASIO, ASD and ASIS) and Schedules 2 and 5 (concerning ASIO).

IGIS noted that the absence of such requirements (which presently apply to similar powers, including in the *ASIO Act*) would present significant difficulties for the effective oversight of intelligence agencies' actions in exercising the new powers. IGIS suggested that all of the new powers should be subject to periodic reporting requirements; as well as 'per use' notifications to IGIS of the conferral and enlivenment of immunities from legal liability in Schedules 1 and 5.[31]

Departmental submission

IGIS understands that the Department considers reporting or notification requirements to be unnecessary in relation to assistance orders under new section 34AAA and civil immunities conferred under new section 21A, principally because reporting is thought to be an additional level of oversight that is reserved for warrant-based activities. The Departmental submission further indicated that 'mandatory reporting for assistance [requests] under 21A is also unnecessary considering its voluntary nature'.[32]

IGIS comments

IGIS continues to support the inclusion of notification and periodic reporting requirements for the reasons given in the IGIS submission and in oral evidence to the Committee.

Facilitation of efficient and effective oversight

Notification and reporting requirements would enable limited oversight resources to be targeted effectively to areas of identified risk in the exercise of coercive and otherwise intrusive powers. In the experience of IGIS, statutory reporting and notification requirements also promote better record keeping practices by agencies about their exercise of powers.

31 IGIS, *Submission 52,* at [1.4], [.1.5], [1.6], [1.9], [2.1.3], [2.2.4], [2.2.7], [5.1.8] and [5.2.6].

32 Department of Home Affairs, *Supplementary Submission 18.3,* p. 19 at [99]-[100].

Reporting (for example, on a warrant operation after it has concluded; or six monthly reports on special intelligence operations) also assists IGIS to develop a comprehensive understanding of the way in which powers are used; how they have assisted agencies in performing their functions; and to identify systemic compliance issues or risks, ideally at an early stage before there is a need for major remedial action.

Existing statutory notification and reporting requirements for similar intrusive powers

The *ASIO Act* currently contains reporting and notification requirements for intrusive powers of a similar nature to those in new section 34AAA (coercive powers) and subsection 21A(1) (powers to confer immunities from legal liability).

Reporting on coercive powers

ASIO's questioning warrants, like section 34AAA assistance orders, enable ASIO to compel people to provide information that assists ASIO in performing its functions. This includes the compulsion of people who are not personally suspected of involvement in activities prejudicial to security (or of being knowingly or intentionally involved).

Reporting on powers to confer immunities

Further, ASIO's special intelligence operations, like subsection 21A(1) assistance requests, involve the conferral of immunities from legal liability on persons who are providing various forms of assistance to ASIO. Both questioning warrants and special intelligence operations are subject to specific notification and reporting requirements.[33]

It is also notable that the *Intelligence Services Act* prescribes specific notification and reporting requirements for the limited circumstances in which the Directors-General of ASIS, ASD and AGO issue emergency authorisations for their agencies to engage in certain intrusive activities in relation to Australian persons. These activities attract the application of immunities from legal liability in section 14 of that Act and section 476.5 of the *Criminal Code*.[34]

Voluntary nature of s 21A(1) requests

The fact that a person's compliance with a request under subsection 21A(1) is voluntary does not diminish the need for IGIS to have an efficient means of visibility over the legality and propriety of the exercise of powers by intelligence agency officials to confer immunities from legal liability. The degree of intrusion into the legal rights of innocent third parties (by removing their rights to legal remedies for loss or injury) is significant, as is the devolution of that power to agency officials.

A person's participation in an ASIO special intelligence operation (in which they are conferred with civil immunity as well as criminal immunity) is also voluntary. However, statutory reporting and notification requirements apply to those operations. These include specific reporting requirements if immunities for causing loss or damage are enlivened, or if statutory limitations are breached.[35]

33 *ASIO Act*, sections 34ZH, 34ZI, 34ZJ (questioning warrants) and sections 35PA and 35Q (SIOs).

34 *ISA,* subsections 9B(4A), (5) and (6).

35 *ASIO Act*, subsection 35Q(2A).

UNCLASSIFIED

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Correspondence ref: OIGIS/OUT/2018/1246 File ref: 2018/140

Mr Andrew Hastie MP
Chair
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600
TOLAbill@aph.gov.au

Dear Chair

Response to a question taken on notice at the public hearing of 27 November

Thank you for the opportunity to appear at the Committee's public hearing on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 on 27 November.

I have enclosed my response to a matter that I took on notice in my answer to a question from Senator McAllister about Schedule 5 to the Bill. This concerns the compliance period for assistance orders under new section 34AAA of the *Australian Security Intelligence Organisation Act 1979* (at pp. 6-7 of the Proof Hansard).

IGIS appreciates the opportunity to participate in the inquiry and would be pleased to provide any further information that the Committee may require.

Yours sincerely

[redacted]

Jake Blight
Deputy Inspector-General

29 November 2018

ENCLOSURE

Response to a question on notice

Compliance period for ASIO's section 34AAA assistance orders (Proof Hansard, 27 November 2018 at pp. 6-7)

Question

Senator McAllister asked some questions of IGIS about assistance orders under new section 34AAA of the *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*) in Schedule 5, and constraints on the period of time in which a person may be required to provide assistance.

> **Senator McALLISTER:** In the case where it's being exercised in conjunction with a warrant, is it the case that, ordinarily, there's a specific time at which everyone understands that a warrant ceases to be in effect?
>
> **Mr Blight:** A warrant has to be served, and then it's exercised. If you're searching a premises, there will be a point at which the search of that premises is finished.
>
> **Senator McALLISTER:** Who makes that decision?
>
> **Mr Blight :** I'd have to take that on notice. There'll be a question of fact, objectively. You couldn't stay for 10 days. The executing officer would effectively have the right to make the decision there.
>
> **Senator McALLISTER:** I'm not concerned with it in general terms. But, if your evidence is that, for the most part, new section 34AAA would be used in conjunction with a warrant—
>
> **Mr Blight** : I think that's [for] ASIO.
>
> **Senator McALLISTER:** and that that in itself presents some kind of time limit, it would be helpful for the committee to understand. It may be that we need to ask that of one of the agencies rather than of you.

We understand that these questions arose from a suggestion of IGIS in submission 52 (at pp. 61-62) that all assistance orders should be subject to the requirement in new subsection 34AAA(3) to expressly specify a compliance period. Currently, the requirements in new subsection 34AAA(3) for an order to specify a compliance period, applies only if a computer or data storage device has been removed from premises under a warrant.

In our supplementary submission 52.1 (at p. 9) IGIS did not agree with a suggestion of the Department of Home Affairs, in supplementary submission 18.3 that, if subsection 34AAA(3) does not apply because a computer or data storage device has not been removed from premises, then 'it is implicit that the person will provide assistance at the time of the warrants executions and in a manner consistent with the issued warrant' (at p. 19). There is nothing in section 34AAA that limits a compliance to the period a warrant is in force and there are legal and practical difficulties in relying on an implied compliance period.

The following response to the question from Senator McAllister also includes some further notes that even if it was possible to imply a compliance period that is the duration of a warrant's execution, that period could be lengthy. For example, while a physical search under a search warrant may be relatively short, that is not the total duration of a search warrant (which for ASIO can be up to 90 days while for police it is 7 days). Furthermore, section 34AAA could be used in conjunction with a range of ASIO warrants including warrants that do not require any physical access to premises such as computer access warrants which can operate for 6 months and enable access to multiple computers repeatedly for that period.

Response

Who makes the decision that the activities authorised under a warrant are complete?

We understand that the executing officer for a warrant is responsible for making the objective factual assessment that the acts authorised under the warrant have been completed.

For example, if a search warrant is issued under section 25 of the *ASIO Act*, one of the acts that may be specified in that warrant is the act of searching the subject premises under paragraph 25(4)(b). In making a factual assessment of whether the act of searching the subject premises was complete, the executing officer would need to assess whether all relevant things or records had been found; or otherwise whether all places on or in the subject premises at which relevant things or records could be located had been searched.

An executing officer must make this factual assessment within the limits of the authority under the warrant. (For example in the case of a search warrant, the search of the subject premises must be completed within the period of effect of the warrant, and in accordance with any conditions specified in the warrant about the conduct of the search, such as any limitations on the time of day or night during which a search may be conducted.)

An executing officer must also act in accordance with the requirements of the *ASIO Guidelines,* including the requirements in paragraph 10.4 with respect to the timeliness, efficiency and proportionality of collection activities. The Committee may wish to seek more detailed information from ASIO about its operational procedures in this regard.

Legal difficulties in using the execution of a warrant as an 'implied compliance period'

As noted in our supplementary submission 52.1 (at p. 9), IGIS is concerned that there would be significant risks in attempting to imply a compliance period into a section 34AAA assistance order based on the period of effect of a warrant, or possibly some kind of sub-set of that period. IGIS remains of the view that it would be preferable, for both compliance and oversight, if all assistance orders were expressly required to specify a compliance period.

In our view, there is doubt that section 34AAA could, as a matter of statutory interpretation, support an implication that the compliance period is the time at which a warrant is executed. The text of several provisions in subsection 34AAA(1) appears to contemplate that information and assistance could be compelled under an order both while a warrant is in force but ***before*** it is executed, and ***after*** a warrant has been executed and ceases to be in force.

Compulsory assistance before a warrant is executed: subparagraphs 34AAA(1)(a)(i)-(iv)

In particular, subparagraphs 34AAA(1)(a)(i)-(iv) appear capable of authorising the issuing of an assistance order which compels a person to provide information to ASIO to enable ASIO to execute a warrant that is in force, before that warrant is executed.[1] In this scenario, the statutory requirement in subsection 34AAA(3) to impose a compliance period does not apply, because there has necessarily been no removal of a computer, since the assistance is compelled in preparation for the execution of the warrant to enable it to be carried out.

---

1 These provisions enable the compulsion of assistance or information that is reasonable or necessary to assist ASIO to access data held in, or accessible from, a computer or data storage device that is: (1) the subject of a computer access, or surveillance device warrant; or (2) is on premises in relation to which a search or surveillance device warrant is in force. These provisions do not require the assistance to be provided ***only*** at the time at which the warrant is executed (that is, the time of doing the things authorised under the warrant).

Consequently, the concept of the execution of the warrant does not appear to provide a cogent basis on which to imply a compliance period for the assistance order in such circumstances, and it is difficult to discern an alternative basis on which an assistance period could be implied.

Compulsory assistance after a warrant has expired: ss 34AAA(1)(b) and (1)(c)(i)-(ii)

Further, paragraph 34AAA(1)(b) and subparagraphs 34AAA(1)(c)(i)-(ii) appear capable of authorising the issuing of an assistance order to compel a person to provide assistance to ASIO by copying or converting into intelligible form data that ASIO has ***already*** lawfully accessed under a warrant, in circumstances in which the warrant itself has expired. (The provisions appear capable of covering circumstances in which the warrant had already expired at the time the assistance order is issued, or if the warrant expires while the assistance order is in force).[2]

In this scenario, the statutory requirement in subsection 34AAA(3) for the assistance order to specify a compliance period would not apply if there was no removal of a computer from premises. This may conceivably occur if the relevant data was accessed remotely under a computer access warrant, or was copied from a computer found on premises entered under warrant. Subsection 34AAA(3) also would not apply if a computer was removed from premises for the purpose of accessing or copying data, and ASIO had then returned the computer while the warrant was in force. In these circumstances, the (completed) execution of the warrant clearly could not provide a basis for implying a compliance period for the assistance order.

Given the potential for assistance orders to be issued in these circumstances, IGIS considers that it would be preferable to avoid relying on an implied compliance period of some kind. Rather, subsection 34AAA(3) could require the Attorney-General to specifically authorise a compliance period for ***all*** assistance orders, not merely if a computer is removed from premises. This would ensure that the Attorney-General is specifically informed by ASIO of the intended compliance period and the supporting case for requesting that period; and is specifically asked to make a decision on its necessity and reasonableness.

In addition to providing clear and certain benchmarks for IGIS oversight of ASIO's requests, this could provide a stronger and more consistent safeguard for persons who are subject to an assistance order, so that they can readily ascertain and understand their obligations and potential liabilities. In the analogous context of statutory notice-based information gathering powers (notices to produce documents, provide information or to attend and answer questions) the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* states that provisions conferring powers to issue such notices should require those notices to 'contain all relevant details' including the time and place of an appearance or the deadline for compliance, as applicable.

The following statement in the *Guide* appears to have equal force with respect to section 34AAA assistance orders:

> Including all relevant details in a notice ensures that a person who receives a notice is aware of his or her legal rights and obligations in relation to the notice. The legitimacy and enforceability of notices to produce

2 These provisions enable the compulsion of assistance or information that is reasonable or necessary to allow ASIO to: (1) copy or data held in or accessible from a computer or data storage device that is the subject of a computer access or surveillance device warrant, or is on premises in relation to which a search or surveillance device warrant is in force; and (2) to convert such data into documentary form or another form intelligible to an ASIO employee or affiliate.

or attend depends on ensuring the rights and obligations of the person served with the notice are clearly outlined.[3]

Practical difficulties in using the execution of a warrant as an implied compliance period for assistance orders under section 34AAA

Even if it was legally possible to imply a compliance period into a section 34AAA assistance order by reference to 'the time of the warrant's execution' as suggested in the supplementary Departmental submission, this may produce unintended consequences.

In particular, it may be very difficult to identify precisely what that period of time would be. Any such period may also be protracted, given the lengthy maximum duration of special powers warrants and the range of activities that may be authorised by those warrants. IGIS considers that there would be benefit, from a compliance and oversight perspective, in avoiding these difficulties by simply requiring all assistance orders to specify a compliance period.

Practical difficulties in relation to search warrants

For example, in the case of search warrants issued under section 25 of the *ASIO Act*, these warrants do not become 'spent' and cease to have effect once a search of the subject premises is completed under paragraph 25(4)(b). Paragraph 25(4)(d) authorises the removal and retention of records and things found during the search for the purpose of inspecting or examining them. The warrant is arguably being executed for as long as those records or things are being examined or inspected in accordance with the warrant while it is in force (up to 90 days).

Uncertainty may therefore arise if ASIO conducted a search of subject premises during which it copied data from a computer on the premises under subsection 25(5) without removing that computer from the premises; and a section 34AAA assistance order then compelled a person to convert that data into an intelligible form. If ASIO had ***also*** removed unrelated records and things that it found in the search of the subject premises, for the purpose of inspecting or examining them, then is it intended that the compliance period for the section 34AAA assistance order is the duration of the remaining examination or inspection activity under the search warrant, since the warrant is still being executed while the examination or inspection is being conducted within the warrant period? If a more limited period is intended, then the basis for identifying that period is unclear.

Practical difficulties in relation to computer access warrants

Further, in the case of computer access warrants, it may be very difficult to identify the 'the time of the warrant's execution' because a single computer access warrant can authorise repeated access to a large number of individual computers and premises while the warrant is in force (for up to six months). A 'computer' within the meaning of section 22 of the *ASIO Act* can cover one or more individual computers, computer systems, computer networks or any combination. It is conceivable that multiple computers may be accessed continuously while a warrant is in force.

Potential for a protracted compliance period

Further, any implied compliance period by reference to the duration of a special powers warrant could be protracted, given the lengthy maximum duration of those warrants. (This is six months

---

3 Australian Government, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, p. 92 at [9.3.3].

for computer access and surveillance device warrants, and 90 days for search warrants). This may create uncertainty about precisely when, within in that period, a person's assistance may be compelled under an assistance order. While new section 34AAA of the *ASIO Act* is modelled on existing section 3LA of the *Crimes Act,* the latter provision operates in relation to law enforcement search warrants that have a maximum period of effect of seven days from the day after issuing. (See subsection 3E(5A) of the *Crimes Act.*)