

UNCLASSIFIED



---

## **Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018**

---

**Submission to the Department of Home Affairs**

The Hon Margaret Stone  
Inspector-General of Intelligence and Security

13 September 2018

UNCLASSIFIED

## Introduction

The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make a submission on the exposure draft of 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 the role and functions of IGIS is provided 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. 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 minor amendments to the Bill and supplementation in Ministerial guidelines. This submission covers the following measures:

- **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 maintain certain technical capabilities for the purpose of being able to provide 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

If the Bill is passed, oversight of the new powers will be complex and resource intensive. The adequacy of IGIS resourcing to maintain effective oversight (including complaint management) will require ongoing monitoring, including as informed by the frequency and manner of use of the new powers by agencies.

## Outline of key issues

<b>Schedule 1—Industry assistance to ASIO, ASD and ASIS .....</b>	<b>3</b>
1.1 Relationship with existing powers and immunities of intelligence agencies .....	3
1.2 Decision-making criteria for issuing requests and notices .....	12
1.3 Conditions of assistance to be provided under a request or notice.....	16
1.4 Immunity from civil liability for acts done under a request or notice .....	18
1.5 Immunity from criminal liability to certain computer offences .....	20
1.6 Attorney-General’s procedures and arrangements for requesting a capability notice.....	22
1.7 Terms and conditions on which help is to be given under a notice .....	23
1.8 Disclosing information about requests and notices for oversight purposes .....	25
1.9 Reporting on intelligence agencies’ use of requests and notices.....	26
<b>Schedule 2—ASIO’s computer access warrants .....</b>	<b>26</b>
2.1 Telecommunications interception powers .....	27
2.2 Temporary removal of computers and other things from warrant premises .....	30
2.3 Concealment of acts or things done under a computer access warrant .....	34
2.4 Disclosure of ‘ASIO computer access intercept information’ to, and by, IGIS officials .....	35
<b>Schedule 5—Other amendments to the ASIO Act .....</b>	<b>36</b>
5.1 Civil immunity for giving voluntary assistance to ASIO.....	36
5.2 Compulsory technical assistance to ASIO in relation to certain warrants.....	43
<b>Attachment A: Role of the Inspector-General of Intelligence and Security .....</b>	<b>49</b>

## 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'<sup>1</sup> may be requested (under 'technical assistance requests')<sup>2</sup> or compelled (under 'technical assistance notices'<sup>3</sup> or 'technical capability notices'<sup>4</sup>) 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'<sup>5</sup> 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.<sup>6</sup> 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.<sup>7</sup> (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.<sup>8</sup> 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.<sup>9</sup>

#### 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*

- 
- 1 New section 317C. (***Designated communications providers*** are 15 types of entities that supply communications-related services, with a nexus to Australia. These include telecommunications carriers, carriage service providers and intermediaries, and various other participants in the communications supply chain. For example, providers of electronic services; device manufacturers; and persons who manufacture, supply, install, maintain or operate telecommunications facilities.)
  - 2 New Part 15, Division 2 (especially new section 317G).
  - 3 New Part 15, Division 3 (especially new section 317L).
  - 4 New Part 15, Division 4 (especially new section 317T).
  - 5 New section 317C. (***Eligible activities*** are defined by reference to each type of communications provider and the communications services that they typically provide to persons within Australia in that capacity. For example, the eligible activities of a telecommunications carrier or carriage service provider are the operation of telecommunications networks or facilities in Australia, or the supply of listed carriage service.)
  - 6 *Inspector-General of Intelligence and Security Act 1986 (IGIS Act)*, subsections 8(1)-(2) and section 9A.
  - 7 *IGIS Act*, sections 8 and 9AA(b).
  - 8 New paragraphs 317G(1)(c)-(d) (requests) and new section 317ZJ (notices).
  - 9 Schedule 1, item 3 (new subparagraphs 476.2(b)(iv)-(vi) of the *Code*).

(*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;<sup>10</sup> proportionality and other requirements in the issuing criteria that limit the conduct able to be authorised;<sup>11</sup> exclusions of certain acts from the immunity;<sup>12</sup> and reporting and notification requirements to IGIS and the Attorney-General.<sup>13</sup>

- The 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,<sup>14</sup> and a limited set of preparatory actions (excluding acts for which ASIO would require a warrant or an authorisation to do in Australia).<sup>15</sup>

The effect of the amendments 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. 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 certain Acts. These include the *Telecommunications (Interception and Access) Act 1979 (TIA Act)*, *ASIO Act* and *ISA*. 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.

---

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

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

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

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

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

15 *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.)

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 or metadata from a carrier or carriage service provider (being activities for which ASIO would require a warrant or an authorisation under the *TIA Act*);<sup>16</sup>
- 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*;<sup>17</sup> 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).<sup>18</sup>

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.<sup>19</sup> However, there are a number of uncertainties and potential gaps in the coverage of this provision, 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.<sup>20</sup> 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*.)<sup>21</sup> 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.

---

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

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

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

19 See also: Explanatory Document, p. 48.

20 New subsection 317ZH(1).

21 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).

IGIS queries whether 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. If there is no such intention, 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. As this type of ambiguity will make oversight more difficult, clarification of this matter would be desirable.

If the words ‘give effect’ 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.<sup>22</sup> 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.<sup>23</sup> 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

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

23 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’.)

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 ... (iv) 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 concealment-related actions generally require authorisation under the relevant special powers warrant, subject to the applicable statutory thresholds and conditions being met.<sup>24</sup>
- 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.<sup>25</sup>

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.

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. One way of facilitating consistent record keeping (and IGIS and Ministerial visibility) would be through amendments to the warrant reporting requirements in section 34 of the *ASIO Act* and section 17 of the *TIA Act*. These

---

24 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).

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



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.

***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 under Division 3 of Part III of the *ASIO Act*.<sup>26</sup> 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(1)(e) and (f) would apply, or are intended to apply, in these circumstances. It is similarly unclear how new paragraphs 317ZH(1)(d)-(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*.)<sup>27</sup> IGIS would support clarification of these matters.

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.<sup>28</sup> 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.

***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.

---

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

27 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].

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

### *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' with the meaning of that term in section 4 of the *ASIO Act*.<sup>29</sup> 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'.)<sup>30</sup>

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.<sup>31</sup> 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*).

Further, a provider who acts in accordance with a 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*.<sup>32</sup> 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).

---

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

30 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*).

31 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)'. 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 (such as the issuing of a notice).

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

### *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 limitation.

#### 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 work to do in relation to notices, given that the agencies which can issue technical assistance notices, or request the issuing of technical capability notices, are ASIO and ‘interception agencies’ (including the AFP and ACIC).<sup>33</sup> 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. 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.<sup>34</sup>

It appears to IGIS that new paragraph 317ZH(1)(e) would apply as follows:

- 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.

#### General 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 Acts listed in new paragraphs 317ZH(1)(a)-(e). 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.<sup>35</sup>

If this is the intended interpretation, then the application of new section 317ZH is likely to be extremely complex, because it would require a review of the application of ***all of the 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.

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).

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

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

35 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.

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

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

- **Potential changes to the substance of Ministerial authorisation requirements from time-to-time due to paragraph 8(1)(b) of the ISA.** Under paragraph 8(1)(b) of the *ISA*, the responsible Ministers for ASIS, ASD and AGO may issue directions that specify the circumstances in which their agencies must obtain a Ministerial authorisation for undertaking activities, in addition to the circumstances prescribed in paragraph 8(1)(a). The substance of any limitation applied by new paragraph 317ZH(1)(e) of the *Telecommunications Act* may therefore change in line with changes to Ministerial directions in force under paragraph 8(1)(b) of the *ISA*. (A similar complexity arises as a result of the statutory function of ASIS under paragraph 6(1)(e) of the *ISA* to undertake certain activities as directed by the responsible Minister.)
- **Complexity arising from the arrangements in Division 3 of Part 2 of the ISA (regarding ASIS assistance to ASIO).** Any limitations imposed by new paragraph 317ZH(1)(e) will have no application to the intelligence production activities that ASIS could undertake without a Ministerial authorisation under Division 3 of Part 2 of the *ISA* for the purpose of assisting ASIO.<sup>36</sup> This means that, if a technical assistance or capability notice purported to require a communications provider to do an act or thing that involved the production of intelligence on an Australian person outside Australia, the application or otherwise of the limitation in new paragraph 317ZH(1)(e) would depend on the precise purpose for which the assistance was to be rendered. If it was for the purpose of assisting ASIO, then new paragraph 317ZH(1)(e) would not apply because ASIS would not be required to obtain a Ministerial authorisation. If, however, the activity was carried out for another purpose, then the limitation in new paragraph 317Z(1)(e) would seem to apply.

These matters would make IGIS oversight extremely complex, and would likely make it impossible for a communications provider to make a meaningful assessment of its legal position under new section 317ZH. Unlike IGIS, a communications provider is unlikely to have access to the necessary information. For example, Ministerial directions given under paragraphs 6(1)(e) and 8(1)(b) of the *ISA* are not legislative instruments<sup>37</sup> and are normally classified. 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*.

---

36 Division 3 authorises ASIS to undertake activities outside Australia that involve the production of intelligence on an Australian person, for the purpose of assisting ASIO. In all other circumstances, ASIS requires an MA to produce intelligence on an Australian person under s 8(1)(a)(i) of the *ISA*.

37 *ISA*, subsections 6(3A) and 8(5).

## 1.2 Decision-making criteria for requests and notices

### 1.2.1 Assessment of proportionality

#### *Technical assistance requests (new s 317G)*

There is no requirement for the Directors-General ASIO, ASD or ASIS (or their delegates)<sup>38</sup> 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.)

In the absence of a statutory requirement, IGIS would assess matters of proportionality and reasonableness in considering the propriety of agencies' decision-making about the making of a request under new section 317G. 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.

However, the insertion of express statutory proportionality requirements in new section 317G, similar to those in new section 317P for technical assistance notices,<sup>39</sup> 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

---

38 See the powers of delegation in new sections 317ZN, 317ZP and 317ZQ. They apply to ASIO affiliates and ASIO employees, and staff members of ASIS and ASD, who hold SES (or equivalent) positions.

39 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'. (But note the comments below, suggesting that more detailed decision-making criteria could usefully be included in new section 317P.)

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 and 317V)*

New section 317P 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, practicableness 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. The concepts of reasonableness and proportionality would cover consideration of the impacts on the provider, as well as potential impacts 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. Equivalent requirements apply to variation decisions under new section 317Q.<sup>40</sup>

It would aid oversight if the Bill, or possibly the *Minister's Guidelines to ASIO* issued under section 8A of the *ASIO Act*, provided more detail on what factors the Director-General of Security or delegate must take into account in applying the criteria under new sections 317P and 317Q. This could promote consistency of decision-making and record-keeping, and provide clear and transparent benchmarks against which IGIS would conduct oversight of issuing and variation decisions.

Equivalent decision-making criteria apply to the Attorney-General in relation to the issuing of technical capability notices under proposed section 317V, and their variation under new section 317X.<sup>41</sup> 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) in relation to new sections 317P and 317Q 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.

### **1.2.2 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, protecting public revenue, or protecting the interests of Australia's national security, foreign relations or national economic well-being.<sup>42</sup>
- ***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

40 New subsection 317Q(10).

41 New subsection 317X(4),

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



provisions, protecting public revenue, or safeguarding national security (but not the interests of Australia's foreign relations or national economic well-being).<sup>43</sup>

### *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*, new sections 317G, 317L and 317T 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 and public revenue-related functions*

The references in new sections 317G, 317L and 317T to agency functions that relate to criminal law enforcement, the enforcement of pecuniary penalties and the protection of public revenue<sup>44</sup> 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.<sup>45</sup> However, 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*.)

IGIS would support clarification of the intended application, preferably in the provisions of new sections 317G, 317L and 317T. Depending on the policy intent, one way of removing ambiguity could be for proposed paragraphs 317G(5)(a)-(c) to provide explicitly that they do not apply to the functions or powers of ASIO, ASD and ASIS. Proposed subparagraphs 317L(2)(c)(i)-(iii) and 317T(3)(a)-(c) could also be amended to provide explicitly that they do not apply to the functions or powers of ASIO. (This might be achieved through the insertion of the phrase 'if the agency is an interception agency,' at the start of each provision mentioned in the previous sentence.)

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

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

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

### 1.2.3 Consideration of multiple coercive powers being exercised against a provider

The decision-making criteria for the issuing of 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.<sup>46</sup> The risk of oppression 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).

Amendments to the statutory requirements of reasonableness and proportionality in decision-making about the issuing of notices in new sections 317P and 317V could provide an effective means of managing this risk, and for IGIS to conduct oversight of this aspect of agencies' decision-making. These provisions could include requirements for the decision-maker to assess the potential for oppression arising from the exercise of multiple coercive powers against a provider (and in the case of technical capability notices, require the requesting agency to provide information to the Attorney-General about 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.

---

46 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.



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

### 1.3.1 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 maximum period of effect of 90 days from when the notice or request was given.<sup>47</sup> Technical capability notices are subject to a maximum period of effect of 180 days from issue.<sup>48</sup>

While there is no limit on the number of new requests and notices that can be issued subsequently, the imposition of a maximum duration effectively requires the periodic re-assessment of the grounds for issuing requests and notices and their specific terms (including consideration of any changes in circumstances). These reviews aid oversight and accountability, and are compatible with most other intelligence warrants and other powers, which have a maximum period of operation, subject to renewal.

However, since there are explicit powers to vary requests and notices in new sections 317JA, 317Q and 317T, there may 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 90 or 180 day maximum (as applicable). This would be consistent with existing provisions of the *ASIO Act* that limit powers of variation in relation to special powers warrants and special intelligence operations.<sup>49</sup>

### 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.<sup>50</sup>

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.<sup>51</sup> However, the acts and omissions of the Director-General of Security (or delegate) in considering whether an assistance notice must be revoked would be subject to IGIS

---

47 New sections 317HA and 317MA.

48 New section 317TA.

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

50 New sections 317R and 317Z.

51 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).

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 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.<sup>52</sup> 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.

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.

### 1.3.4 Limitation in the prohibition on creating 'backdoors' (new s 317ZG)

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.<sup>53</sup> It also prohibits these notices from preventing a provider from rectifying any existing 'backdoors' that it may identify.<sup>54</sup> 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.<sup>55</sup> Notices are of no effect to the extent that they purport to impose such requirements on a provider.<sup>56</sup>

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,<sup>57</sup> and would be taken to have been authorised for the purpose of the computer offences in Part 10.7 of the *Code*.<sup>58</sup>

---

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

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

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

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

56 New subsection 317ZG(5).

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

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

(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.<sup>59</sup>

IGIS queries whether requests are intended to be utilised in this way. 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). 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 any such requests.

## 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.<sup>60</sup> The existing immunity from civil liability conferred on participants in ASIO's special intelligence operations also includes explicit limitations and exclusions.<sup>61</sup> 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

---

59 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.

60 Schedule 5, item 2 (new paragraphs 21A(1)(d) and (e) of the *ASIO Act*).

61 *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.

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.<sup>62</sup>

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*.

#### 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 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.

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.<sup>63</sup> 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.

---

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

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

## 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.<sup>64</sup>

### 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.<sup>65</sup>

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 particular:

- **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.<sup>66</sup> 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.<sup>67</sup> 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.<sup>68</sup> 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.<sup>69</sup>

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

65 Without such a limitation, 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 (namely, the computer offences in Part 10.7 of the *Code*). It is not clear that the issuing of a notice would necessarily enliven the defence of lawful authority in section 10.5 of the *Code*.

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

67 *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 of a computer must be reported to the Attorney-General in warrant reports: *ASIO Act*, subsection 34(2). See [1.9] below.

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

69 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

- **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;<sup>70</sup> and certain preparatory acts done within Australia, provided that ASIO would not require a warrant to carry out those acts.<sup>71</sup> 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.<sup>72</sup> 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*.<sup>73</sup>

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. Nor does the authorisation in item 3 appear to exclude instances in which the provider is reckless in relation to the circumstance that a notice had no legal effect because of the application of new section 317ZG or 317ZH. If there is no intention for item 3 to provide an authorisation in respect of compliance with a legally ineffective notice, then it may 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:

---

special intelligence operations) and section 10A of the *ISA* (reports by ASD and ASIS in relation to Ministerial authorisations).

70 *Code*, subsection 476.5(1).

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

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

73 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’.

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

Consideration might be given to expressly limiting the power of these agencies to make technical assistance requests,<sup>74</sup> 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 noted 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 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.<sup>75</sup> IGIS would conduct oversight of ASIO's compliance with those procedures and arrangements in making requests for the issuing of capability notices. However, neither the Bill nor

---

74 The making of requests by ASIO, ASD and ASIS in these circumstances would raise matters of propriety. 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.

75 New subsection 317S(1).



the existing provisions of the *IGIS Act* contain a 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. Further, as determinations made under new section 317S are not legislative instruments<sup>76</sup> 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.

IGIS is therefore supportive of 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.<sup>77</sup> 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.)<sup>78</sup> Other conditions include a default requirement for the parties submit to arbitration of the terms and conditions of compliance, if they cannot reach agreement.<sup>79</sup>

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.<sup>80</sup> An equivalent power is conferred on the Attorney-General in relation to technical capability notices.<sup>81</sup> 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 *Telecommunications Act*; the imposition of a regulatory burden on the provider; and the reasons for the giving of the notice.<sup>82</sup> 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.

---

76 New subsection 317S(4).

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

78 New subsection 317ZK(3).

79 New subsection 317ZK(4).

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

81 New paragraph 317ZK(e).

82 New subsection 317ZK(2).



### 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. 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.

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. Ready access to written records of decisions, supporting reasons, and the information on which they are based, will be essential to such oversight.

### 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.)<sup>83</sup>

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.

---

83 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.)

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.<sup>84</sup> 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.<sup>85</sup>

### 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.<sup>86</sup> 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).

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)*.

---

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

85 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).

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

### 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).

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*.

### 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.

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.

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.

## 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;<sup>87</sup>
- temporarily remove a computer or other thing from premises, for the purpose of doing any thing specified in the warrant;<sup>88</sup> and
- 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.<sup>89</sup>

IGIS has identified some opportunities to make technical and other minor adjustments to various provisions to ensure that there are no unintended barriers to effective oversight of the new powers. In particular, IGIS has identified several ambiguities in the proposed provisions, which could be clarified legislatively. 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*.<sup>90</sup>

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

---

87 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).

88 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).

89 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).

90 *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).

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’,<sup>91</sup> the ‘security matter’<sup>92</sup> or ‘foreign intelligence matter’<sup>93</sup> in respect of which warrants can be issued, and the applicable issuing thresholds. 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).<sup>94</sup> 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. IGIS will continue to have oversight of the legality and propriety of warrant requests (including the underlying intelligence case) and the conduct of warrant operations.<sup>95</sup> However, the proposed powers may be framed more broadly than what is necessary to achieve this intended outcome.

---

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

92 *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.)

93 *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 legal and natural persons including bodies politic, entities or other things such as activities or events.)

94 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.

95 *IGIS Act*, subsection 8(1) and section 9A.

*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’<sup>96</sup> 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) and 27E(2).

It is unclear whether the conferral of such power is intended. The circumstances in which TI powers might be thought necessary to gain entry to premises are not immediately apparent. The conferral of TI powers in relation to such activities 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. 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 paragraphs 27E(2)(c) and (d).

*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, 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. 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.

---

96 ASIO Act, paragraph 25A(4)(a), subsection 27A(1) and paragraph 27E(2)(c) (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).



### 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*.

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).<sup>97</sup>

### 2.2.1 Purpose of temporary removal

The explanatory document 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).<sup>98</sup> However, the 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.

97 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).

98 Explanatory document, p. 57.

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. Accordingly, 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 indefinite) period of time.

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. Or, 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. (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.

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.



### 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 most persons in conducting their ordinary, lawful business and personal affairs, that deprivation could reasonably be regarded as likely to be a *material* interference with, or interruption or obstruction of, their lawful use of the computer in many cases.) In this event, the limitation in 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.

### 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

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.)

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. 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.<sup>99</sup> 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. 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.<sup>100</sup> 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.<sup>101</sup> 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;<sup>102</sup>
- 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

99 *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).

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

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

102 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).

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;<sup>103</sup>

- 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);<sup>104</sup> 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 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).<sup>105</sup>

## 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).<sup>106</sup> 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

103 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.

104 *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).

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

106 Items 7, 8 and 12.

period. 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.

### 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.

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. If so, 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).

## 2.4 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.<sup>107</sup>

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.<sup>108</sup> The Bill also proposes to insert new section 63AC, which authorises permitted dealings with ‘ASIO computer access intercept information’.<sup>109</sup> 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.<sup>110</sup>

IGIS assumes that this is an unintended omission. 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*. All that would change as a result of the proposed amendments to the *ASIO Act* in Schedule 2 to the Bill is that this information would be obtained under a different type of warrant (namely, a computer access warrant).

107 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’).

108 Schedule 2, item 125,

109 Schedule 2, item 124.

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

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. Accordingly, IGIS seeks the inclusion of an exception in new section 63AC for disclosures to, and by, IGIS officials.

## 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*.<sup>111</sup> 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).<sup>112</sup>

#### 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. The Attorney-General must specifically authorise an operation as an SIO, the relevant conduct to be undertaken in that operation, and the participants.<sup>113</sup> SIOs may only be authorised in relation to a sub-set of ASIO's statutory functions.<sup>114</sup> 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).<sup>115</sup>

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.<sup>116</sup> 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.<sup>117</sup>

---

111 Schedule 5, item 2.

112 Schedule 5, item 1.

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

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

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

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

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

### 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, such as sources, become 'ASIO affiliates' (within the meaning of that term in section 4 of the *ASIO Act*).<sup>118</sup> If ASIO were to adopt a practice of using new 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). 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.

---

118 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).)

### 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.<sup>119</sup> However, an advisory recommendation is clearly of lesser value to an aggrieved person than a legally enforceable remedy.

### 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.

### 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 questions about how requests made under subsection 21A(1) will interact with existing warrant or authorisation requirements.

#### *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.

---

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



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 intelligence directly from the computer or 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 intelligence. 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).

#### *Possible amendment to prevent bypassing of warrant or authorisation requirements*

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;<sup>120</sup> a maximum 90-day period of effect for requests;<sup>121</sup> and express provisions governing variation.<sup>122</sup>

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 pay close attention to ASIO's decision-making about the use of new subsection 21A(1) in these circumstances.

### 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.<sup>123</sup> It is also in contrast to the proposed maximum period of 90 days for technical assistance requests under new subsection 317HA of the *Telecommunications Act*.

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 (90 days).<sup>124</sup> 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, 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.

---

120 New subsection 317H(2).

121 New paragraph 317HA(1)(b). See also new section 317J (request for performance in a specific period, and on specified conditions)

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

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

124 New paragraph 317HA(1)(b).

### 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 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 subsection 317H(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.

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).

#### *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 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.<sup>125</sup> IGIS would be assisted by clarification of the intended source of a power to vary or revoke subsection 21A(1) requests.

---

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

### *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. For these reasons, IGIS is likely to pay close attention to the exercise of powers by the Director-General or delegates under new subsection 21A(1); and to the Director-General's decision-making in exercising the power of delegation in new subsection 16(1A).

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).

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);
- 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 rendering 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.<sup>126</sup>

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 may add complexity to the task of conducting oversight.

### 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 bodies corporate and bodies politic*

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 notice 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?

---

126 New subsection 34AAA(1).

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'.)

This broader application of new section 34AAA of the *ASIO Act* may be unintended, noting that the justification given in the explanatory document 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).<sup>127</sup> 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.

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.)

---

127 Explanatory document, p. 111.

### 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;<sup>128</sup> and any other conditions determined by the Attorney-General.<sup>129</sup>

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. 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.

### 5.2.3 Form of orders and requests for orders

New section 34AAA does not prescribe the form in which orders or requests for orders must be made (for example, in writing or orally in defined circumstances). Nor does it prescribe any record-keeping requirements equivalent to those in subsection 32(4) for special powers warrants. The application of equivalent statutory parameters to new section 34AAA would assist oversight, since these orders operate in combination with special powers warrants.

### 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

---

128 New paragraphs 34AAA(a) and (b).

129 New paragraph 34AAA(c).

technical assistance and capability notices.<sup>130</sup> 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.

### 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.<sup>131</sup> 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, and the broad classes of persons in relation to whom a notice may be issued.<sup>132</sup>

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.

---

130 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).

131 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].

132 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.



### 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 document address this scenario. IGIS supports clarification of this matter.

#### *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. This would be assisted by a statutory requirement for ASIO to include information about previous orders and requests for orders in relation to a person in its requests under section 34AAA, 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. 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 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.

## 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 currently has 27 staff.

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.<sup>133</sup> 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.<sup>134</sup> 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.<sup>135</sup>

---

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

134 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).

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