UNCLASSIFIED

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

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

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

Dear Chair

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

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

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

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

Yours sincerely

[redacted]

Jake Blight
Acting Inspector-General

13 February 2018

1 National Circuit BARTON ACT 2600 Phone [redacted]

UNCLASSIFIED

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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