Australian Government
Department of Home Affairs

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

Parliamentary Joint Committee on Intelligence and Security

Supplementary Submission

Introduction

1. This supplementary submission, provided to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Act), addresses matters raised in the submissions of the Inspector-General of Intelligence and Security (IGIS) and Commonwealth Ombudsman (the Ombudsman). Both the submission of the IGIS and the Ombudsman reiterate recommendations made by both bodies to the PJCIS's previous inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill), which concluded on 5 December 2018.
2. All five Schedules of the Act are intended to implement a clear policy objective: to ensure that Australia's national security and law enforcement agencies have the tools to investigate serious crime and gather critical intelligence and information in the digital age. Oversight is an important part of this framework and ensures the functions of agencies, already bounded by statute, are discharged according to law. The significant amendments made to the Bill in December 2018 strengthened oversight powers and allow for meaningful oversight without disproportionately hampering the legitimate exercise of agency activities.
3. The Department understands that the terms of reference for the present inquiry are primarily concerned with the implementation of the Act and review of the Government amendments introduced and passed on 6 December 2018. The Government fully supported the recommendations made by the PJCIS in the *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (the PJCIS Report). The IGIS and the Ombudsman submissions discuss their previous recommendations that are in addition to those that were the subject of specific recommendations in the PJCIS report.
4. This submission focuses on how the Government amendments moved on 6 December 2018 incorporate the IGIS and Ombudsman recommendations that were the subject of specific recommendations in the PJCIS report. This submission also analyses the additional IGIS and Ombudsman recommendations, as discussed in their submissions to this current PJCIS inquiry.

Government amendments made to address IGIS and Ombudsman concerns

5. The Government made extensive amendments to the then Bill on 6 December 2018 in response to the PJCIS Report. The majority of these 167 amendments were in response the Committee recommendations 4, 5 and 12, which went directly to strengthening IGIS and the Ombudsman's oversight of the powers and significantly refining independent scrutiny across all Schedules of the Bill. The Government addressed PJCIS recommendations 4, 5 and 12 in full and additional amendments were made in response to further recommendations by both the IGIS and the Commonwealth Ombudsman. How recommendations 4, 5 and 12 were addressed, and the additional amendments, are discussed below.
6. **The Government implemented in full Committee recommendation 4**, which recommended that the Bill be amended to incorporate suggestions from the Ombudsman to establish a clear inspection authority for the Ombudsman and allow for notification and information sharing requirements to complement the inspection activities of State and Territory oversight bodies.

7. Section 317ZRB was introduced to establish a clear and robust authority for the Ombudsman to inspect, at their discretion, the records of an interception agency (the Australian Federal Police (AFP), State and Territory police and the Australian Criminal Intelligence Commission (ACIC)), gather information in that inspection and submit a report on inspections for tabling in Parliament.
8. Paragraph 317ZF(3)(g) and subsection 317ZF(5A) now include explicit authority for the Ombudsman to receive and share information about Schedule 1 powers consistent with their functions and duties. Subsections 317ZF(5B), 317ZF(5C) and 317ZF(12B) – 317ZF(12D) now allow for clear disclosure to the inspecting authorities of State and Territory interception agencies. These amendments remove impediments to the smooth exchange of information for the purposes of oversight in all relevant jurisdictions.
9. **The Government implemented in full PJCIS recommendation 5**, which recommended that the Bill be amended to incorporate suggestions from the IGIS on Schedule 1 powers, specifically including:
    - explicit notification and reporting requirements when issuing, varying, extending or revoking a notice or request under Schedule 1
        - Approximately **39** Government amendments gave affect to this recommendation.
    - limits on the exercise of Schedule 1 powers (including extending prohibition on systemic weaknesses to voluntary notices, ensuring decision-makers consider necessity and intrusion on innocent parties)
        - Sections 317ZH, 317ZAA, 317JC and 317RA were comprehensively amended to incorporate this recommendation.
    - defences for IGIS officials, and
        - Additional amendments to section 317ZF make explicit that the IGIS and the Ombudsman do not bear an evidential burden in unauthorised disclosure offences.
    - clear information sharing provisions.
        - Section 317ZF now explicitly ensures that information may be shared to the IGIS, Ombudsman and relevant State and Territory oversight bodies to ensure that they can conduct meaningful oversight of the powers.
10. **Consistent with PJCIS recommendation 12,** the Department continues to monitor implementation of the Act and will have detailed discussions with oversight bodies as the new regime is implemented and the additional measures are utilised.
11. Additional to the amendments made to give effect to the Committee's report, a number of other significant measures were adopted to improve oversight and incorporate ancillary recommendations by the IGIS and Ombudsman and to strengthen safeguards. These include:
    - Requiring that, when issuing a technical assistance notice (TAN), issuing agents advise providers of their right to complain to the Ombudsman or the IGIS, as the case may be.
    - Ensuring that, in the course of existing inspections of records under the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004* the Ombudsman can inspect, and report on, the exercise of Schedule 1 powers.
    - Consistent with recommendations from the IGIS, providing decision-makers the ability to exercise discretion about which elements of the public interest exception to full compensation or arbitration processes are included in the process of settling terms and conditions in section 317ZK.

- Extending express decision-making and proportionality requirements for the issue of voluntary technical assistance requests (TARs).
- Requiring Schedule 1 information to be included in classified annual reporting under the *Australian Security Intelligence Organisation Act 1979.*
- Improving annual and warrant reporting for sections 21A and 34AAA powers.
- Requiring that sections 34AAA and 21A requests are made in written form, or that written records will be made of oral requests, except in limited circumstances.
- Establishing notification requirements to the IGIS for the issue of section 21A requests.
- Establishing that a section 34AAA order must be revoked where the grounds on which the order is made cease to exist.
- Amending sections 63AB and 63AC of the *Telecommunications (Interception and Access) Act 1979* to ensure that IGIS and the Ombudsman officials have a clear avenue to communicate information about intercepted material associated with ASIO and law enforcement computer access warrants.
- Ensuring that, if a person suffers a loss or injury as a result of the exercise of law enforcement computer access powers, the Commonwealth is liable to pay compensation.
- Ensuring that the Ombudsman is notified of any concealment activities undertaken by a law enforcement agency pursuant to a computer access warrant.
- Ensuring the limitation on material interference or material loss or damage applies to concealment activities for computer access warrants.
- Requiring things removed for examination pursuant to a computer access warrant be returned to premises after a reasonable time has elapsed.
- Placing significant periodic reporting obligations on the Director-General for concealment activities.

12. In summary, all PJCIS recommendations that relate to the IGIS and the Ombudsman were adopted in full. Additional amendments were made to the Bill consistent with discussions held between the IGIS, the Ombudsman, and the Department, and to facilitate their oversight functions.

Additional IGIS and Ombudsman recommendations

13. The IGIS and Ombudsman submissions discuss their recommendations additional to those that were the subject of specific recommendations in the PJCIS report. **Attachments A** and **B** to this submission analyse these additional IGIS and the Ombudsman recommendations.

Conclusion

14. The Government adopted all PJCIS recommendations, including those pertaining to the oversight functions of the IGIS and Ombudsman. The Department welcomes the opportunity to analyse additional recommendations by both oversight bodies.

Attachment A

Recommendations of the Commonwealth Ombudsman	
Recommendation	**Comments**
That subsection 317ZRB(7) be removed from the Act **Note: Subsection 317ZRB(7) provides that before tabling the copy of the report from the Ombudsman, the Home Affairs Minister may delete from the copy information that, if made public, could reasonably be expected to prejudice an investigation or prosecution, or compromise any interception agency's operational activities or methodologies.**	On 6 December 2018, in correspondence to the Committee, the Ombudsman noted that the discretion of the Minister for Home Affairs to delete material that could reasonably be expected to prejudice an investigation or prosecution, or compromise an interception agency's operational activities or methodologies in subsection 317ZRB(7) is inconsistent with other statutory reporting requirements and the Ombudsman's broader role Section 317ZRB provides the Ombudsman with broad power to inspect interception agency records and report on outcomes from that inspection. Given the sensitive capabilities, relationships and methodologies that Schedule 1 powers may cover, subsections 317ZRB(4) and 317ZRB(7) were inserted to ensure that any public report did not include information that would compromise investigations or agency activities. The threshold is high and exclusion is only warranted in serious circumstances; where inclusion could reasonably be expected to prejudice an investigation or prosecution or compromise operations. The Department notes the Ombudsman comments that reports generally relate to records that have ceased or expired, avoiding any risk to ongoing operations. Schedule 1 powers are not traditional warrants issued for the investigation of persons of interest and necessarily tied to investigations and, accordingly, the circumstances of cessation and expiry and the role of Ombudsman oversight, are unique. The powers deal in the information exchange between Government and industry and go to matters of ongoing commercial sensitivity and capability protection, which, given the nature of the regime, may not be isolated to one interception agency. The risk of jeopardising both confidential industry information and the protected information across multiple agencies may be significant and justifies additional safeguards. These Ministerial exclusion powers have precedent in other reporting regimes, some overseen by the Ombudsman. For example, in recognition of the sensitivity of information relating to

	control orders, subsection 61(4) of the *Surveillance Devices Act 2004* requires that the Minister must exclude information that is classified as 'control order information' from any inspection report before it is laid before each House of Parliament. Such exclusions are also a feature of ASIO classified annual reporting under subsection 94(4) of the *Australian Security Intelligence Organisation Act 1979,* noting that subsection 94(5) allows the Minister to delete items from a report tabled in parliament if publication would be prejudicial to security, among other factors. Noting the above, the Department recognises the Ombudsman's important, and independent, oversight role and welcomes Committee consideration of other avenues to minimise the risk of compromising capabilities and jeopardising key relationships. Agencies have expressed the constructive relationships they enjoy with the Ombudsman and conditional vetting undertaken jointly by the Ombudsman and the agency may be an appropriate alternative.
That the term "by name or otherwise" be more clearly defined in section 27D(1)(b)(ix) of the SD Act	The inclusion of the language 'by name or otherwise' recognises the fact that there may be instances where a person cannot be specified by name. Increasingly, the relevant particulars of a person for the investigation of online criminality, or criminality facilitated by computers, are electronic signatures such as IP addresses. The phrase 'or otherwise' accounts for this common occurrence.
That the expression 'earliest time' used in section 27E(7)(k) is reconsidered	The term, 'earliest time' is necessarily undefined to account for common instances where, in the circumstances, concealment activities cannot be conducted within a 28 day period. It is not uncommon for a relevant device to be moved, taken overseas, disabled or otherwise made unavailable to law enforcement for months, or even years. In these cases, no concealment can take place. While the Ombudsman correctly notes that computer access warrants may be extended for 90 days, it is not uncommon for concealment activities to occur over years. A person may reactivate a device a significant time after an initial warrant is in place, alerting authorities to the need for concealment. In these circumstances, it is impracticable to seek continual renewal of warrants.

That the limitations applied to TANs and TCNs in section 317ZH also apply to TARs	This suggestion is already reflected in the Act.

Attachment B

Recommendations of the Inspector-General of Intelligence and Security	
Recommendation	**Comments**
That there be annual reporting requirements in Schedule 1 for ASIS and ASD	The powers in Schedule 1 of the Act available for use by ASIS and ASD are limited to technical assistance requests (TARs) for specific objectives related to the functions of these agencies. TARs are a voluntary power that cannot compel assistance from any entity. However, their use can be captured within the existing annual reporting scheme in sections 42 and 42A of the *Intelligence Services Act 2001*. These sections require the Director-General of each organisation to give a report to the Minister of agency activities for the year, while some matters are prescribed for inclusion in the report, there is significant discretion as to what other information could be included. As a matter of good administrative practice, this report can be expected to include the number of TARs each agency issued during that year. Ministerial directions, such as a direction by the Finance Minister under section 105D of the *Public Governance, Performance and Accountability Act 2013*, can be issued to ensure that information about TARs is included in the annual reports of these organisations.
That there be a requirement for notification of IGIS if a provider causes significant loss	All intelligence and security agencies are expected, and in ASIO's case required, to report on the use of TARs, technical assistance notices (TANs) and technical capability notices (TCNs) in their classified annual reporting. The Department has recommended to ASIS, ASD and ASIO that these reports note instances where the agency is aware that a provider has relied on the immunities and significant loss or damage has been incurred by a third party. Ministerial directions, such as a direction by the Finance Minister under section 105D of the *Public Governance, Performance and Accountability Act 2013* or legislative instruments made under subsection 94(2C) of the *Australian Security Intelligence Organisation Act 1979* can be issued to ensure these facts are included in the

	annual reports of these organisations.
That there be an express requirement to consider impact of immunity on all third-parties	In addition to whether a request or notice is **reasonable**, **proportionate, practicable** and **technically feasible**, a decision-maker is required to consider an extensive list of 8 factors, these are: • the legitimate interests of the relevant provider • the legitimate expectations of the Australian community relating to privacy and cybersecurity • the objectives of the notice • the availability of other means to achieve the objectives of the notice • where the requirements are the least intrusive known forms of industry assistance in relation to persons who are not of interest to the agency • whether the requirements are necessary • the interests of national security • the interests of law enforcement These decision-making criteria directly address a wide range of considerations that go to the impact of a TAN, TAR or TCN on third parties. In a particular, reasonableness, necessity and proportionality are expansive concepts that capture considerations of third-party impact. As the IGIS noted in their first submission to the PJCIS "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". The Department brings the Committee's attention to 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.
That there be a fixed maximum period of effect for TARs.	The Department has received advice that this recommendation is unworkable. TARs may be used to deploy technical capabilities over long periods. Given the voluntary nature of TARs, any period of cooperation longer than the default 90 days can only occur with provider cooperation and a

	good working relationship with the agency. Placing an artificial ceiling upon a relationship of voluntary cooperation is only likely to frustrate both agencies and industry. The period of time will need to be considered on a case-by-case basis with the agreement of both the provider and industry.
That there be a statutory clarification of overlap between TARs and ASIO21A(1) requests	The distinction between the assistance available under TARs and ASIO's section 21A(1) of the ASIO Act power to request voluntary assistance under Schedule 5 of the Act is clear on the face of the legislation. Primarily this distinction is provided by the comparatively narrow availability of TARs against the broader availability of the section 21A(1) power; TARs only applying to the activities listed in section 317E and to the defined category of designated communication providers. By contrast, the section 21A(1) power is available where the Director-General of Security is satisfied the person or body's conduct meets the broad objectives and restrictions of the ASIO Act. It remains unclear what the benefit of further drawing out this distinction may be, particularly given they are voluntary powers that will be utilised distinctly and to the awareness of both the IGIS and the relevant person. The Department refers the Committee to its response to this concern as outlined in its supplementary submission 18.3 to the review into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (see page 16).
That there be further limitations on types of damage covered by civil immunities	IGIS's suggestions to limit civil immunities to exclude conduct causing serious financial loss, damage to property, personal injury or harm, or an offence would, in the Department's view, limit the utility of the industry assistance powers. When providers are asked to provide assistance to law enforcement or intelligence agencies, it is essential that they are able to avail themselves of appropriate immunities. This is a central guarantee of the regime and recognises the value that Australia's agencies place on good faith cooperation with industry members. While immunities under the distinct power in section 21A have some qualifications of immunity provided, these immunities are not accompanied by the broader safeguards attached to TARs, TANs and TCNs. For example, the significant decision-making thresholds that must be met – assistance must be assessed as reasonable and proportionate – as well as additional constraints on the powers, appropriately bound the exercise of the immunities. It is highly unlikely that a decision-maker could be satisfied that conduct which causes serious financial loss, damage or

	personal injury – or any of the other identified harms – would meet these decision-making criteria. The Department contends this is an appropriate balance to strike and important flexibility to preserve in the Act.
That criminal immunities are brought into line with those available to agencies	The criminal immunities to computer offences in the *Criminal Code* attached to things done in accordance with a TAR, TAN or TCN is an important safeguard for providers who are assisting Government. These immunities extend the logic already inherent in the *Criminal Code* immunities that persons who are acting in accordance with a legal instrument, like a warrant or authorisation, are not liable for the activities consistent with the authority of that instrument. The relevant members of industry are intimately involved in the lifecycle of data and operation of computers within Australia - it is particularly important that these immunities are available to the particular species of provider that fall within the definition of designated communications provider. These are not blanket immunities, they are tied to the conditions of the TAR, TAN and TCN which themselves are limited in a significant way by the Act's safeguards. Section 317ZG ensures that any activity cannot jeopardise the broader security of data and section 317ZH ensures that a TAR, TAN and TCN cannot replicate a warrant or authorisation. That is to say that what can be listed in each instrument is already significantly restricted by the current warrant and authorisation regime and the need for those agencies to attain assistance through those channels instead of, or in addition to, a TAR, TAN or TCN. Where a provider acts in accordance with a TAR, TAN or TCN, they should not be criminally liable for this valuable assistance, even if there are defects in the original request. TARs have since been included in the prohibition in 317ZH, which narrows the criminal immunity available under a TARs. In effect this, as suggested by the IGIS submission, treats voluntary compliance and mandatory compliance in a similar manner.
That there be a statutory requirement to give section 317S procedures	Procedures under section 317S are intended as administrative processes to centralise and coordinate the use of TCNs within and between jurisdictions. The IGIS has significant powers to review any such procedures under their inspection function within section 9A of the *Inspector-*

for making TANs to IGIS	*General of Intelligence and Security Act* and may inquire about procedures that relate to ASIO and TCNs at a given time. This, in addition to the already extensive notification and information sharing regimes established for oversight bodies. The IGIS is currently able to conduct oversight of ASIO's compliance with any procedures established under section 317S where they relate to ASIO. Further, a TCN may be requested by multiple agencies across jurisdictions that are not within the remit of the IGIS. Accordingly, jurisdictional considerations must be taken into account.
That there be a requirement for ASIO warrants to identify if industry assistance powers were used to facilitate execution of warrants	As in the case of the previous recommendation, access to this information could be obtained by IGIS through their general inspection function or the multiple legislative pathways for oversight provided by the Act. These avenues can be used to examine this information, and combined with the record-keeping requirements on ASIO, already offer a means to scrutinise any interaction between industry assistance measures and ASIO warrants.
That section 317ZH is expressly limited to only warrants in force	The words 'assist in, or facilitate in, giving effect to a warrant', consistent with other statutory language in section 313 of the *Telecommunications Act 1997,* go to doing things that support a warrant in force. Ordinary meaning of the words make clear that it is not about discharging the 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 the warrant itself. In any case, agencies do not operate under extant warrants. These are provisions enacted for the avoidance of doubt and, as such, their scope to meaningfully narrow the limitation in 317ZH(1) is remote.
That there be a clarification on whether industry assistance powers offer 'standing' or 'one-off' assistance	TARs and TANs are designed to respond to both single occasion assistance and standing assistance. Their terms may be set flexibly, consistent with what is reasonable, proportionate, practicable and technically feasible. Agencies and providers may determine if one mode of assistance is more appropriate to a situation when the assistance is sought. Restricting the powers to a single instance of assistance may necessitate having the Director-General or chief officer undertake a decision-making process repeatedly for assistance that would be better represented by a period of conduct.

	The IGIS notes at 1.3.3. that this suggestion is relevant in the absence of fixed statutory maximum period of effects. Given that the Government amendments introduced fixed statutory maximum periods of effect of 12 months for TANs, the Department considers that these concerns may be alleviated.
That section 317ZH applies to TARs issued by ASD or ASIS (s 317ZH)	As the Department noted at paragraph 45 in its primary submission to this inquiry, the *Intelligence Services Act 2001* (IS Act) does not include relevant authorisations or warrants. Unlike a warrant, ministerial authorisations in the IS Act cannot require a provider to do anything (like hand over data for example), rather they authorise ASIS and ASD to undertake independent activities. In any case, the provision in section 317ZH is drafted in a broad manner ('a law of the Commonwealth') to capture authorisations and warrants additional to those available in the most relevant Acts that are identified in subsection 317ZH(1). The Department appreciates the IGIS's identification of a technical oversight in section 317ZH(4).
Schedule 2	
That warrant reporting requirements are extended to temporary removals (s 34)	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.
Schedule 5	
21A	
That there be statutory issuing criteria requiring the Director-General of Security (or delegate) to be satisfied that the conferral of civil	This requirement is taken from the *Minister's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence),* (10.4(a)). These ministerial guidelines are given under subsections 8A(1) and 8A(2) of the ASIO Act to be observed by ASIO in the performance of its functions. To require a proportionality test is likely to be unnecessary as any means used to obtain information (including by way of assistance

immunity is reasonable and proportionate (s 21A(1)	to provide information) must be proportionate to the gravity of the threat posed and the probability of its occurrence.
That there be a statutory exclusion of certain conduct causing serious loss or harm (s 21A(1)	The civil immunity is not extended to conduct which would amount to an offence against a law of the Commonwealth, a State or a Territory. Commonwealth, State or Territory offences could capture conduct that involves physical or mental harm or injury. This is in addition to the limitation on immunity for conduct that results in significant loss of, or serious damage, to property. The policy intention is to cover pure economic loss and conduct resulting in physical or mental harm or injury within the immunity. This would be consistent with a plain reading of the section and the current operation of similar powers such as section 35K of the ASIO Act.
That there be a statutory maximum period of effect for section 21A(1) requests (s 21A(1)	It is difficult to set particular maximum periods of effect under section 21A(1) given the broad conduct that the civil immunity scheme is intended to cover. The Department considers that a maximum period is unnecessary as the immunity arises out of the '*conduct*' applicable to the particular request by ASIO.
That there be an exclusion of conduct that could be the subject of a TAR under Part 15 of the Telecommunications Act (s 21A(1)	IGIS's concerns above regarding TARs in Schedule 1 address this issue. Schedule 5 is designed to be broader in scope than the persons from whom assistance can be sought. TARs covers designated communications providers, whereas section 21A covers persons or bodies. This recognises the broader application of section 21A that may be able to assist ASIO in the performance of its functions that may not necessarily be technical in nature. As noted above, there may be instances of assistance that could be addressed by the use of either power. However, the distinction comes down to the fact that TARs, unlike the section 21A(1) power, form part of a broader industry assistance framework and their presence within this framework provides the most useful context to explain their purpose. Further clarification can be found in the Act's Explanatory Memorandum, the Department's previous submissions (see supplementary submission 18.3 to the first Committee inquiry) and may be delivered through administrative guidance if this becomes necessary.
That there be an exclusion of conduct for which ASIO would require a warrant or an	This recommendation of the IGIS assumes that section 21A of the ASIO Act could be utilised to require persons or bodies to undertake activities that would otherwise require ASIO to obtain a warrant or authorisation. Including a specific restriction that ASIO cannot request a person or body to engage in conduct that would require ASIO to obtain warrant or authorisation as if an ASIO

authorisation to undertake directly (s 21A(1)	officer was undertaking those actions is very likely to have significant unintended consequences. There are three counterpoints to consider against the recommendation of IGIS: • Section 21A specifically limits any conduct to ensure that it does not involve the commission of an offence. Given that warrants are only utilised to overcome illegality associated with the actions they authorise, there are very limited instances in which the circumstances contemplated by this recommendation could arise. This recommendation is limited to circumstances where the activity requested under section 21A would only be unlawful if exercised by an ASIO officer, and not by the person or body requested to complete the activity. • Including a legislative exclusion for those limited circumstances would have significant unintended consequences for the expected functions of ASIO. For example, voluntary assistance is a key aspect of human intelligence – legislating a restriction on circumstances where warrant regimes would apply to gathering of information by law enforcement and intelligence agencies that would not necessarily apply to civilians may prohibit ASIO from gathering essential intelligence, and • Excluding these instances may force ASIO to utilise more intrusive powers to achieve outcomes ordinarily done through voluntary means Voluntary assistance by members of the public (including bodies) is important to national security agencies in gathering intelligence information to prevent national security incidents/serious crime and a key aspect of human intelligence gathering activities. There may be instances where law enforcement and national security agencies would ordinarily require a warrant or authorisation but a member of the public may not require a warrant or authorisation to undertake conduct. For example, an ASIO officer could not enter a premise without lawful authority (e.g. a search warrant, or consent from an individual) for the purposes of assisting ASIO in the performance of its functions. However, a human intelligence source may be able to enter a private property in which they have authority to do so without a warrant and have a conversation with a person of interest. Restricting requests for persons or bodies to engage in conduct which only ASIO could complete without a warrant would significantly hamper the collection of human intelligence and create significant barriers to the investigation of serious security concerns.

	An additional impact from the above example may be that, where ASIO is limited from requesting voluntary assistance, ASIO may be required to use more intrusive powers, such as the exercise of questioning powers or search warrants on premises. By restricting voluntary assistance (which specifically prohibits the conduct of any illegal activity, and only renders civil, and not criminal, immunity) ASIO would be required to conduct more intrusive activities, contrary to the expectations outlined in the Ministerial Guidelines.
That there be a requirement for notification of IGIS if conduct causes serious harm or damage (s 21A(1)	Existing oversight mechanisms sufficiently permit oversight of this aspect of the regime. In the event that this notification requirement is introduced into the regime, care should be taken to consider the Department's response to the above under '*Exclusion of certain conduct causing serious loss or harm*'.
That there be a specific statutory power of variation or revocation (s 21A(1)	The power to vary and revoke a decision is inherent in the decision-making power under section 21A by virtue of 33 of the *Acts Interpretation Act 1901*.
That there be clarification on whether requests can cover the repetitive provision of assistance (s 21A(1)	It is intended that section 21A voluntary assistance provisions apply flexibly, including to both repetitive provision of assistance, and single instances. The Department views that conduct could involve a range of activities and restricting it to a single instance of assistance may necessitate having the Director-General undertake a decision-making process repeatedly for assistance that would be better represented by a period of conduct rather than a single instance of civil immunity.
34AAA	
That section 34AAA is amended to include an activity that is prejudicial to security where the underlying warrant, of an unrelated security matter, is issued (s 34AAA)	The drafting of section 34AAA ensures that there is a nexus between the recommendation to issue an order under subsection 34AAA(1), and the issuing of the assistance order under subsection 34AAA(2) by the Attorney-General. In other words, subsection 34AAA(2) empowers the Attorney-General to issue an order upon the Director-General's recommendation which is based on whether the criteria in subsection 34AAA(1) have been met. Paragraphs 34AAA(2)(b) and (c) relate to the broader functions of ASIO in relation to security. Specifically, subparagraph 34AAA(2)(c)(i) allows for requests to specifically target persons of interest who are suspected of being involved in activities that are prejudicial to security. This appropriately limits the use of assistance orders to circumstances where the Attorney-General is

	satisfied that the assistance to be provided by a person relates to a risk that can reasonably cause harm to Australia and the Australian community. This is a high threshold and ensures that the assistance powers will only be used to support the legitimate work of ASIO. Given the seriousness of potential acts that are prejudicial to security, it is critical that ASIO be able to compel assistance from persons suspected of involvement. There are many ways in which involvement may be made out, but these should be viewed through the lens that there are many people with relevant knowledge that can ensure the discovery and safe resolution of activities that represent a material threat to the Australian public. For example, assistance can be sought from persons that are unintentionally acting as a conduit for activities that are prejudicial to security, or provide services to another person, which enables activities that are prejudicial to security.
That all orders, including ASIO's computer access warrants, are required to specify essential matters (s 34AAA)	The requirement to '*specify essential matters*' relates to subsection 34AAA(3) which provides additional requirements for circumstances where the relevant computer or data storage device is not located on the premises that is specified in the warrant in force. Additional transparency is 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. These circumstances do not fundamentally change the warrant or provide the basis for ASIO to conduct activity beyond the warrant, but provides the specified person with appropriate details given the change in location. The remote access of computers and devices under computer access warrants are subject to significant safeguards and transparency measures. These include the high thresholds prescribed by the statutory criteria for the issuing of warrants and the exercise of powers under them, the requirement for the Minister to issue warrants, the Director-General's reporting requirement and the independent oversight role of the IGIS. This ensures computer access warrants are issued only where appropriate and necessary, and are oversighted by the highest level of authority for such matters.
That there be statutory safeguards against arbitrary deprivations of liberty (s 34AAA)	It is not the intention of the powers under section 34AAA in compelling a specified person to assist ASIO to be the basis for deprivation of liberty or inhumane treatment. Appropriate oversight and robust safeguards support these measures and ensure that requests are only issued where necessary. This matter was raised in detail as part of a previous Departmental supplementary submission to

	the PJCIS's previous inquiry in December 2018. The Attorney-General, upon a determination of the reasonableness and necessity of an order, issues assistance orders. The Attorney-General is the chief law officer of the Commonwealth and has the authority, experience and knowledge to consider the reasonableness and necessity of the assistance orders. The Attorney-General is also in a position to consider other factors not provided for in section 34AAA including human rights issues. For example, it is entirely reasonable for the Attorney-General to reject an application for the issuance of a request on the basis that it may adversely affect the human rights of a person, unreasonably interfere with a person's privacy or impact a person that does not have the ability to understand or meet the request. Additionally, the power to make orders under section 34AAA is significantly fettered by the requirement that the Attorney-General be satisfied on reasonable grounds that the access will substantially assist the collection of intelligence as set out in 34AAA(2). It is unlikely that the Attorney-General could be satisfied of this standard if the order required ASIO to indefinitely detain and violate the rights of the specified person or otherwise harm their human dignity. The legislation also includes safeguards to protect persons who are unable to comply with an assistance order. Specifically, paragraph 34AAA(4)(b) provides that a person who is not capable of complying with a requirement in the order does not commit an offence.
That there is a requirement for the Director-General of Security to delete records 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 (34AAA)	As standard practice, ASIO appropriately protects information obtained in the course of their work. This could be addressed through Ministerial Guidelines.
That there is an obligation on the	The intention of the assistance orders is to support warranted activities or ASIO functions that may impact security. As a result, the existence of an assistance order is inherently linked to the

Director-General of Security to take all necessary steps to cease executing a section 34AAA order, if satisfied that the issuing grounds have ceased to exist (s 34AAA).	timeframes of a warrant or ASIO operation. The Department and ASIO are open to addressing this issue through Ministerial Guidelines.
That there is a statutory requirement for the notification and service of assistance orders on persons (s 34AAA)	The issuance of an assistance order under section 34AAA is subject to annual reporting requirements. This ensures that the Minister and Parliament are able to scrutinise the amount of assistance orders issued. The IGIS currently have the ability to scrutinise the operation of section 34AAA and are able to obtain information, take sworn evidence and enter agency premises to assist with their oversight functions.
That there is 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 (s 34AAA)	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 and detention warrant or questioning warrant. These separate regimes may be individually exercised against a single individual for legitimate investigative purposes as each seeks to obtain different types of evidence from a subject and carries unique incentives to comply. It is contemplated that other coercive powers, such as search warrants, be exercised against the subject of a questioning and detention warrant or a questioning warrant. Further, there is no in principle reason to prevent the exercise of multiple coercive powers where this serves an investigatory need. IGIS already plays a significant role in administering questioning and detention warrants and questioning warrants, able to be present throughout an entire questioning session and recommend the suspension of questioning in response to any concerns. Additionally, IGIS's general oversight function will allow them to audit both of these powers and any interaction between them should this occur. As such, the Department does not consider separate statutory guidance necessary to provide IGIS further access to the use of these powers. The Department is also working with IGIS in considering the current operation of questioning and detention warrants and questioning warrants in response to the PJCIS Review of the operation, effectiveness and implications of Division 3 of Part III of the *Australian Security Intelligence Organisation Act 1979* (ASIO's questioning and detention powers).