Submission

to the

Parliamentary Joint Committee on Intelligence and Security (PJCIS)

Review of the

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

22 January 2019

Joint submission by:

Communications Alliance
Australian Industry Group (Ai Group)
Australian Information Industry Association (AIIA)
Australian Mobile Telecommunications Association (AMTA)
Digital Industry Group Inc (DIGI)
Information Technology Professionals Association (ITPA)

NOTE: ***nbn™ is a member of Communications Alliance, the Ai Group and the AIIA but has not been involved in the preparation of this submission.***

ASSOCIATIONS

Communications Alliance* is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through Industry self-governance.

The **Australian Industry Group (Ai Group)*** is a peak industry association in Australia which along with its affiliates represents the interests of more than 60,000 businesses in an expanding range of sectors including: manufacturing, engineering, construction, automotive, food, transport, information technology, telecommunications, call centres, labour hire, printing, defence, mining equipment and supplies, airlines, and other industries. The businesses which Ai Group represents employ more than one million people. Ai Group members operate small, medium and large businesses across a range of industries. Ai Group is closely affiliated with more than 50 other employer groups in Australia alone and directly manages a number of those organisations.

The **Australian Information Industry Association (AIIA)*** is Australia's peak representative body and advocacy group for those in the digital ecosystem. AIIA is a not-for-profit organisation that has, since 1978, pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment and drive Australia's social and economic prosperity.

AIIA's members range from start-ups and the incubators that house them, to small and medium-sized businesses including many 'scale-ups', and large Australian and global organisations. While AIIA's members represent around two-thirds of the technology revenues in Australia, more than 90% of our members are SMEs.

The **Australian Mobile Telecommunications Association (AMTA)** is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile network operators and carriage service providers, handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry.

The **Digital Industry Group Inc (DIGI)** is a not-for-profit industry association representing the digital industry in Australia. DIGI includes representatives from Amazon, Facebook, Google, Oath, and Twitter. DIGI members collectively provide digital services to Australians including Internet search engines, online stores and other digital communications platforms.

The **Information Technology Professionals Association (ITPA)** is a not-for-profit organisation established to advance the understanding of ICT matters within the community, corporate and government sectors in Australia.

IPTA's members are professionals within the IT Industry in Australia and abroad who aim to advance the practice of Information Technology as a profession.

IPTA's vision is for its members to deliver outcomes which enhance and enrich society through the understanding and application of technology in an increasingly online world.

NOTE:** ***nbn™ is a member of Communications Alliance, the Ai Group and the AIIA but has not been involved in the preparation of this submission.

1. Introduction

The Associations and their members are grateful for the opportunity to provide further input to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (Act).

As we have stated publicly during 2018, we remain appreciative of the valuable and diligent work undertaken by the Committee to date throughout its Inquiry and, in particular, the way that the Committee remained focused on its task, despite the political pressure and, at times, extraordinary circumstances that have attended the scrutiny and passage of the legislation.

Our submission seeks to take account of the recommendations made by the PJCIS in its December 2018 *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*.

The submission offers comments and suggestions in relation to the Government amendments to the Bill that were passed by both Houses of Parliament on 6 December 2018.

We urge the Committee to consider recommendations for improvements to the Government amendments that were passed on 6 December 2018 and to many other remaining problematic aspects of the legislation.

As was manifestly clear in the lead-up to the relevant sittings of the House of Representatives and the Senate, the Government amendments were drafted in haste in an overnight session and were distributed only in the early hours of 6 December. Almost inevitably, there remain, in our view, significant problems with the amendments and other elements of the legislation. Many of the amendments are difficult to understand or interpret, appear unlikely to remedy the problems identified by Industry and/or exhibit omissions which need to be addressed.

In drafting this submission, we have drawn on a range of sources, including the views of the Associations' members who have been involved in our scrutiny of the legislation (dating back to the initial consultation of the draft Bill).

We have also drawn on what we see as the most useful and constructive elements of the proposed Labor amendments (that were withdrawn during debate in the Senate on 6 December) in order to address some of the remaining problematic aspects of the Act.

In addition, the Associations reiterate their concern that the impact of this Act on the exporting activities of Australian Industry security and encryption products, that is now captured by the definition of 'designated communications provider', has not been sufficiently considered. The geopolitical impact of the Act must be further interrogated, and particular attention should also be focused on the legal and economic implications of the application of the law on Australian Industry.

Furthermore, the ability of Government and business to access international security and encryption products may also be impacted making both Australian businesses and Government agencies vulnerable to cyberattack and data breaches. It is unclear how this will be monitored and addressed.

2. Suggested Amendments

The Associations commend the PJCIS and Government for the changes that have already been incorporated into the Act. Many of those changes assist in strengthening the request/notice scheme and provide additional clarity. However, the Associations recommend that the Act be further amended to ensure that the far-reaching powers afforded in the legislation are only applied where necessary and within clearly defined boundaries which take into account the potentially competing requirements of security/safety for the purpose of law enforcement and crime prevention, the rights of designated communications providers and their employees, the security/safety of electronic products and services and, consequently, the cybersecurity and privacy of all Australians – and indeed the Internet at large.

We recommend that the following amendments be incorporated into the legislation as soon as possible, i.e. prior to the statutory review of the legislation by the Independent National Security Legislation Monitor. Please also refer to the table further below for a more detailed list of suggested amendments and for further explanations of the items listed in the bullet points below.

- Enshrine into the legislation a warrant-based system with judicial consent to Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs) and their respective variations. It is only appropriate that the far-reaching powers granted by the legislation are supervised by an eligible judge. The fact that a person has been given the authority to issue a warrant does not guarantee sufficient oversight and/or independence in this context and must, therefore, be complemented by judicial consent.

  We support the amendments in relation to a warrant-based system with judicial consent as tabled by Labor on 6 December 2018.

- It appears very difficult to adequately define the terms 'systemic weakness/vulnerability' and 'target technology'. As currently drafted in the Act, these definitions are difficult to understand, ambiguous and are significantly too narrow. The limitations intended to be given to systemic vulnerability/weakness through the definition of target technology do not achieve the desired objective. Specifically, it is unclear what constitutes a class of technology, (e.g. would a 'class' be all mobile handsets, or Android phones, but not iPhones, or the mobile handsets offered by one service provider but not another, or some other combination of factors?). Assuming this term has a common-sense meaning (to the extent this exists), then the application to the whole class of technology creates a far too narrow characterisation of what constitutes a systemic weakness or vulnerability.

  Consequently, we recommend deleting the definitions of systemic weakness/ vulnerability and target technology and, instead, to more clearly and narrowly articulate in Section 317ZG the prohibited effects of a TAN or TCN. We note the limitations contained in Section 317ZG but maintain that the definitions of these three terms are not useful and/or significantly too narrow to be acceptable.

  We support the amendments to Section 317ZG as tabled by Labor on 6 December 2018.

- The threshold for using the powers afforded in the legislation is very low, i.e. the legislation can be applied in the context of preventing or investigating criminal offences that carry a prison sentence of 3 years. When assessing this threshold, it becomes clear that relatively minor offences compared to the crimes originally contemplated to be combatted by the legislation (terrorism, child abuse, human trafficking etc.) can be captured by this definition. For example, under the *Crimes Act* a prank or menacing phone call could satisfy the 3-year prison sentence criterion. Consequently, we strongly recommend raising the threshold for offences which could give rise to the powers of the Act being used. The *Telecommunications (Interception and Access) Act 1979* (TIAA) already contains a definition of 'serious offence' in Section 5D. The general threshold set by that section is an offence punishable by imprisonment of life or for a period, or maximum period, of at least 7 years. The term 'serious offence' should have only one

meaning between the *Telecommunications Act 1997* and the TIAA. The existing original definition in the TIAA is appropriate and should be adopted.

- The consultation requirements for TANs and TCNs ought to be strengthened. It appears that many of the requirements can easily be avoided by the requesting agency simply stating that the request is urgent (something that it is easy to imagine agencies would almost invariably do). Further, the processes underlying the consultation requirements are somewhat unclear and/or mean that effective consultation can be bypassed.
- The inclusion of an assessment of whether a TCN may be contravening Section 317ZG is a welcome addition. However, the provisions must be significantly strengthened to achieve the desired effect of allowing for an independent and qualified third opinion. Therefore, the legislation should be amended so that the Commonwealth Ombudsman or another independent authority (instead of the Attorney-General) is to appoint the two assessors (or a panel), and only after having invited nominations for candidates from Industry and Government.

  It is also key that both assessors come to the same conclusion that a TCN is not in breach with the limitations placed on notices, in order for the Attorney-General to be allowed to give the notice. A mere consideration of the report produced by both assessors is inadequate.
- The list of matters that the Minister must have regard to when considering the approval of a TCN or of a variation of a TCN is less extensive than the consideration that must be given for TARs, TANs and variation of TANs. This is insufficient given the extended powers granted by a TCN. Importantly, the Minister should be required to give consideration to the legitimate expectations of the community regarding privacy and cybersecurity and whether the requested thing is the least intrusive means of achieving the agency's objective. The respective provisions in Section 317TAAA and 317XA ought to be brought in line with 317J and 317RA.
- Some of the above suggestions highlight that the delineation between TANs and TCNs is complex and ill-formulated throughout the legislation. It seems that the actions requested by a TAN could be used to the same effect as a TCN but would then not be subject to the same scrutiny. Consequently, we suggest – as we have done in previous submissions to the PJCIS – removing the entire concept of TANs altogether from the legislation. This would not reduce the powers available to agencies but would reduce complexity and eliminate some of the shortcomings that stem from a rather artificial delineation between TANs and TCNs.
- The legislation aims to ensure that it cannot be used to bypass the mandatory data retention or interception legislations. However, those protections are largely eroded by two loopholes:
    a. one that allows agencies to make requests and notices, including those that have the effect requesting actions that would usually be governed by the data retention or interception legislations, if they facilitate giving effect to a warrant. This loophole must be eliminated, and we recommend the removal of Sections 317H(4) and (5).
    b. a second loophole arising from the fact that 'listed acts or things' include 'installing, maintaining, testing or using software or equipment' and there is no limitation placed on the functionality that could be deployed within the system of a provider by installing and maintaining software or equipment nominated by an agency. For example, the software or equipment may give the agency direct access to metadata or information or the software or equipment might allow the agency to control or operate a system or service independently of the designated communications provider. (Also refer to item 19 in the table below.)

These loopholes also erode the special protections for journalists in the data retention legislation, under which a special journalist warrant is required to obtain the metadata relating to journalists.

- The legislation only creates a defence for providers if the act requested by a TAN or TCN is done in a foreign country and would contravene foreign law. However, for example, if an Australian provider took action in Australia that compromised the security or privacy of a European citizen under the *General Data Protection Regulation* (GDPR) of the European Union, the provider could be liable for fines of up to 4% of its global revenues, thereby placing the provider into an extremely difficult position with respect to compliance with either legislation.

  Therefore, the implications for a provider of complying with the Act ought to be an express consideration when assessing the reasonableness of a TAN/TCN, and the defence afforded by the legislation ought to be extended to include actions taken in Australia as well as in a foreign country.

<table>
<tr><th>No</th><th>Section</th><th>Subject</th><th>Comment</th><th>Suggested alternative drafting</th></tr>
<tr><td>1</td><td>Independent National Security Legislation Monitor Act 2010
4B, (1D)(b)</td><td>Review of the Act by INSLM</td><td>• Limit the review timeframe to avoid late commencement of review and review dragging on.</td><td>• Agree with suggested Labor amendment as per motion, i.e. omit “as soon as practicable after” and replace with “before the end of”.</td></tr>
<tr><td>2</td><td>317B</td><td>Def. electronic protection</td><td>• This is not a definition but a clarification of what can be included in the term. It should be made clear that electronic protection can include far more than authentication and encryption.
• The inclusion of this reference to the term ‘electronic protection’ does not clarify the practical scope of the term which remains problematic particularly in Section 317ZG.</td><td>• We seek deletion of the phrases ‘into a form of electronic protection’, "in a form of electronic protection’ and ‘in relation to a form of electronic protection’ where ever they occur in 317ZG. The use of the term ‘electronic protection’ in 317ZG creates an additional qualification that limits the benefit and scope of 317ZG.</td></tr>
<tr><td>3</td><td>317B</td><td>Def. serious Australian offence</td><td>• The threshold of imprisonment of 3 years sets a significantly too low bar. Some examples from the Criminal Code Act 1995:
<table>
<tr><td>Interference with political rights and duties; s 83.4(1)</td><td>Imprisonment: 3 years</td></tr>
<tr><td>Equipping one's self to commit theft or a property offence; s 132.7(1)</td><td>Imprisonment: 3 years</td></tr>
<tr><td>Using a carriage service to menace, harass or cause offence; s 474.17(1)</td><td>Imprisonment: 3 years</td></tr>
<tr><td>Improper use of emergency call service; ss 474.18(1)-(2)</td><td>Imprisonment: 3 years</td></tr>
</table>
• The Telecommunications (Interception and Access) Act 1979 (TIAA) already contains a definition of ‘serious offence’ in Section 5D. The general threshold set by that section is an offence punishable by imprisonment of life or for a period, or maximum period, of at least 7 years. The term ‘serious offence’ should have only one meaning between the Telecommunications Act 1997 and the TIAA.</td><td>• We recommend adopting the definition of serious offence that is used in Section 5D of the Telecommunications (Interception and Access) Act 1979 (TIAA).</td></tr>
</table>

4	317B	Def. systemic vulnerability, systemic weakness, target technology	• These definitions are very difficult to understand, ambiguous and appear significantly too narrow. The limitations intended to be given to systemic vulnerability/weakness through the definition of target technology do not achieve the desired objective. • Specifically, what constitutes a class of technology? Assuming this term has a common-sense meaning (to the extent this exists), then the application to the whole class of technology is far too narrow. Consider the case where ASIO instructs screen capture technology be introduced into all smart phones produced by one large android manufacturer but not all android smart phones. Arguably, this means that not the whole class of technology is affected and, therefore, the modification would not constitute a systemic weakness or vulnerability. • We note the limitation contained in 317ZG but maintain that the definitions of these three terms are not useful and/or significantly too narrow to be acceptable.	• Remove all three definitions and amend the limitations in 317ZG(4A-C) as per suggested Labor amendments to ensure adequate protections. • Agree with suggested Labor amendment as per motion on 317ZG.
5	317E	Listed acts or things	• The already extremely wide range of listed acts or things (LATs) has now been extended to also include anything that assists or facilitates giving effect to a warrant or an authorisation under law. It is not clear why this is required. • We note that 317ZH(4) and (5) contain similar provisions which should equally be deleted to avoid an even further expansion of LATs and the circumstances when those can be requested. Also refer to item 19.	• Delete 317E (1)(da)
6	317H(4); 317M(5); 317MAA(6) 317TAA; 317JA; 317Q; 317TAA; 317XA	Record of oral Technical Assistance Request (TAR), Technical Assistance Notice (TAN) and Technical Capability Notice (TCN)	• The requesting person only needs to retain the record that has been made of a request/notices that has been orally given while that request/notice is in force. This appears to be too short to allow for adequate scrutiny if this was required at a later stage. • 317MAA(6) does not require the relevant agency to also provide a written record of the advice within the specified timeframe to the provider. • The obligation to keep a record of an orally given variation of a TAR is missing. • The obligation to keep a record of an orally given variation of a TAN is missing. • The obligation to keep a record of an orally given TCN is missing. • The obligation to keep a record of an orally given variation of a TCN is missing.	• Retain records for 3 years after the expiry of the request/notice. • Include an additional requirement as a new 317MAA(6)(b) to provide the provider with the written record of the advice within the same 48 hours. • Include an equivalent obligation for variations of TARs as a new 317JA(5A). • Include an equivalent obligation for variations of TANs as a new 317Q(5A). • Include an equivalent obligation for TCNs as a new 317TAA(4). • Include an equivalent obligation for variations of TCNs as a new 317XA(3A). • Include a requirement to always also provide written advice in the same timeframe to the provider in line with the suggested amendment above.

7	317ZK(3)	Compliance costs	• 317ZK(3) grants the right to compensation of reasonable costs but does not provide any guidance as to how such costs would be established. The Explanatory Memorandum (p. 70, para. 276) already anticipates that the actual compliance costs may not be deemed reasonable. • The right to compensation ought to include a right to compensation for damage to the network etc. which is a direct result of compliance with the request/notice. • The arbiter for a designated communications provider who is not a Carrier or Carriage Service Provider is the AG him/herself, thereby introducing a risk for bias.	• Remove 'reasonable' to ensure that providers are paid the cost of compliance. • Extend the right to compensation to damage incurred as a result of compliance. • Make the arbiter for non-Carriers/CSPs the Commonwealth Ombudsman or an authority likely to be less biased than the AG.
8	317L(2)(a)	Delineation of TAN and TCN	• It appears that 317L(2)(a) attempts to draw a line between a TAN and a TCN. This should be done more clearly.	• Amend to "A technical assistance notice has no effect to the extent (if any) to which it would require a designated communications provider to be capable of giving help if the provider is not already able to provide such help. "or similar. • However, we recommend the removal of TANs throughout the legislation, refer to item 22.

9	317PA(2) and (3); 317W(3); 317Y(3)	Consultation requirements for TAN and TCN: urgency	• The requirement to consult (in the case of TANs) or the time allowed for consultation (TCNs and variations of TCNs) can be very easily avoided/shortened by citing urgency. This is a very low bar as it can be expected that a majority of notices and their variations may be considered urgent by the requesting authority. • It is also not clear how consultation on TCNs would be facilitated in case the consultation period was shortened significantly and to the effect that meaningful consultation is no longer possible. • Importantly, even during a shortened period the provider has the right to request an assessment, and the timeframe for completion of that assessment and report can be after the expiry of the shortened consultation period. The AG, however, cannot proceed with the giving of a TCN without having regard to the report. • 317W(7) and (8) address circumstances in which it is proposed to issue a TCN that has the same, or substantially the same, requirements imposed by another TCN that was previously given to the provider. In these circumstances, the AG does not have to give the provider a written notice setting out the proposal and inviting them to make a submission on the proposal but only needs to 'consult' the provider. o What is the nature of the consultation the AG must undertake; and o If the provider now has the capability because they were required by the first TCN why would a further TCN seeking the same requirements be needed at all? Should not a TAN now be the appropriate Notice? If the provider still does not have the capability, then an extension of the original TCN under 317TA ought to be the appropriate action.	• Clearly define the requirements for consultation for TANs. • Clearly define the circumstances of urgency with a high threshold. • Clarify the arrangements for the production of an assessment and report in a case of urgency. However, this must not result in the waiver of the right to request an assessment. Consider a minimum period for consultation and conclusion of the assessment process that cannot be reduced even in circumstances of urgency. • It is not clear what case scenario would necessitate 317W (7) or (8). They would seem to be superfluous provisions and outside the legislative scheme for TANs and TCNs. Delete those sections and, consequently, 317W(9).
10	317Q	Consultation requirement for variations of TAN	• The requirement to consult on a proposed variation of a TAN is missing.	• Insert consultation requirements equivalent to (amended) 317PA.
11	317TAAA; 317XA	Approval of TCN; Approval of variation of TCN	• 317TAAA(1) ought to include a reference that a TCN cannot be given unless 317W and 317WA have been complied with. • 317TAAA(3) does not require the AG to also provide a written record of the approval within the specified timeframe to the provider. • 317XA(1)(a) ought to include a reference that a variation of a TCN cannot be given unless 317Y and 317YA have been complied with.	• Include additional reference as new 317TAAA(1)(c). • Include an additional requirement as a new 317TAAA(3)(b) to provide the provider with the written record of the approval within the same 48 hours. • Include additional reference as new 317XA(1)(a)(iii).

12	317TAAA; 317TXA	List of matters for consideration when approving TCN	• The list of matters that the Minister must have regard to when considering the approval of a TCN or of a variation of a TCN is less extensive than the consideration that must be given for TARs, TANs and variation of TANs. This is not acceptable given the extended powers granted by a TCN. Importantly, the Minister must give consideration to the legitimate expectations of the community regarding privacy and cybersecurity and whether the requested thing is the least intrusive means.	• Amend 317TAAA(6) and 317XA(6) in line with 317J and 317RA.
13	317W(7) and (8)	Renewal of TCN	• 317W(7) negates the requirement to issue a consultation notice to the provider and to consider submissions if the TCN is essentially the same as the immediately preceding TCN. However, 317W(8) then stipulates that the Attorney-General (AG) must consult the provider if the TCN is essentially the same as the immediately preceding TCN but gives no further details as to what the consultation requirements are. The two sections appear contradictory and require clarification and detail around the consultation requirements.	

14	317WA; 317YA	Assessment and report of TCN/variation of TCN	• The appointment of the two assessors is made by the AG and is, therefore, likely to be biased. • In addition, 317WA/317YA does NOT stipulate that the assessors have to be independent, i.e. the AG could appoint a member of ASIO as the technical expert. • Information provided by AustCyber suggests that Government is already in the process of identifying a panel (as opposed to two) of technical experts/retired judges. If there was to be a panel, it is not clear whether all panel members would provide their opinion or just two selected members. It would be assumed that the panel consists of equal numbers of technical experts and retired judges. • It is not clear if the appointed assessors would be appointed for a specified, longer term or on a case by case basis. • 317WA(11)/317YA(10) only requires the AG to "have regard to the copy of the report". This offers no protection for providers and it is likely that the findings in the report are being 'overridden by national security concerns' as already evidenced during the consultation process in the drafting stage of the Bill. • It is also unclear how the AG is to proceed if the two assessors disagree on the assessment whether the TCN would contravene 317ZG. Given the importance of the independent review, the AG ought not be allowed to proceed with the notice unless both assessors come to the conclusion that the notice satisfies all criteria of 317WA. This also removes the issues of how the AG is to 'have regard to' the report. • It is not appropriate to give the greatest weight to the contravention of 317ZG.Other criteria, such as using the least intrusive measure, may have equal or greater weight than the contravention of 317ZG.	• Amend 317WA(2)/317YA(2) for the Commonwealth Ombudsman to appoint the two assessors (or a panel), and only after having invited nominations for candidates from industry and Government. • Clarify the term of the appointment. • In case of a panel, ensure equal numbers. • Include requirement of independence of the two assessors into 317WA(4) and (5)/ 317YA(4) and (5). • Amend 317WA(11)/ 317YA(10) to the effect that the AG must not give a TCN unless the two assessors come to the conclusion that all criteria of an amended 317WS(7) (refer to suggested Labor amendments) have been satisfied.

15	317ZB; 317RA; 317ZAA	Breach of foreign law	• The legislation only creates a defence for providers if the act requested by a TAN or TCN is done in a foreign country and would contravene foreign law. However, for example, if an Australian provider took action in Australia that compromised the security or privacy of a European citizen under the General Data Protection Regulation (GDPR) of the European Union, the provider could be liable for fines of up to 4% of its global revenues, thereby placing the provider into an extremely difficult position with respect to compliance with either legislation. Therefore, the implications for a provider of complying with the Act ought to be an express consideration when assessing the reasonableness of a TAN/TCN, and the defence afforded by the legislation ought to be extended to include actions taken in Australia as well as in a foreign country.	• Include into 317RA and 317ZAA, respectively, the legal implications for a provider of complying with the requirements of a TAN/TCN as a mandatory consideration when considering the reasonableness of the TAN/TCN. • Remove 'in a foreign country' from 317ZB(a) and (b).
16	317ZF	Unauthorised disclosure of information	• Employees of providers must not disclose TAR/TAN/TCN information. Government claims that the corporate entity, i.e. the designated communications provider, is the recipient of the request/notice. However, the Act itself does not specify this be the case and instead uses 'person' in its definition of a provider. • It is also not clear how employees of a provider can share information internally in order to comply with the request/notice. It appears from the Explanatory Memorandum that 317ZF(3)(a) is intended for this purpose but this ought to be made clearer within the legislation itself.	• Clarify that the recipient of a request/notice must be the CEO, MD etc. of a provider and that where this is not the case, the recipient is permitted to share the information with management of the provider. • Amend 317ZF(3)(a) to clearly state that employees of a provider can share the information, including with parties external to the provider, to the extent this is required to comply with the request/notice.

17	317ZG(4)	Limitations regarding systemic weaknesses etc.	• 317ZG(4)(A) and (B) refer to a weakness/vulnerability that is "selectively introduced to one or more target technologies that are connected with a particular person". This may suggest that a physical communications connection is required for the reference to apply. • 317ZG(4)(A) and (B) refer to "information held by any other person". The use of 'held' creates a too narrow application as it does not include, e.g. the damaging or disabling of a system, destruction and damaging of data that is not being held and real time system data that is created by not held. • 317ZG(4)(C) defines the circumstances of (A) and (B) "if the act or thing creates a material risk that otherwise secure information can be accessed by an authorised person". The use of 'accessed' in this context appears too limiting. It is conceivable that information is not being accessed by yet be made less secure through other means. It is also conceivable that the flow-on consequences from the weakness only enables or facilitates access at a later time as vulnerabilities may not be detected immediately even though it is likely that they will be detected later-on.	• Use Amendment as suggested by Labor
18	317ZGA	Limits on TCN	• 317ZGA only applies to TCNs. Given the intent of this section and the extremely wide scope of LATs (317E), 317ZGA must be amended to also apply to TARs and TANs. • 317ZGA(1)(c) artificially limits the notice that can be made to "the capability to enable communications […] be intercepted in accordance with an interception warrant" (emphasis added). It appears that any capability to intercept communications ought to be excluded not only those in accordance with a warrant. • 317ZGA(3) only applies to information to be kept or caused to be kept. This clause ought to also apply to information being disclosed as the disclosure ought to be managed through the *Telecommunications Act 1997*. • 317ZGA(4) replicates Section 187A(4)(b) of the *Telecommunications (Interception and Access) Act 1979* (TIAA). Given the intent of the section if would be preferable to also put beyond doubt that content and substance of a communication cannot be kept (and disclosed, see above) using the powers of a request or notice.	• Amend 317ZGA to equally apply to TARs, TANs and TCNs. • Delete reference to interception warrants in 317ZGA(1)(c). • Include 187A(4) of the TIAA into 317ZGA(4).

19	317ZH	General limits on TAR, TAN, TCN	• 317ZH(1) ought to expressly list the *Telecommunications Act 1997* as it is one of the key Acts that is being used to request metadata. • The protections afforded by the limitations set out in 317ZH(1) to (3) are largely being eroded by the exceptions contained in 317(4) and (5) if a request or notice would assist in, or facilitate, giving effect to a warrant or authorisation under law. This is an incredibly low bar in any situation but also erodes the special protections for journalists in the data retention legislation (warrant required). An interception agency just needs to obtain a warrant for a suspect/source, and any form of protection for any designated communications provider (and journalist for that matter) no longer applies as the listed act or thing can be declared as facilitating giving effect to a warrant. • The protections afforded by the limitations set out in 317ZH(1) to (3) are also ineffective to the extent that they fail to take into account the possibility that an agency will have direct access to the provider's systems, services or information by reason of requiring installation or maintenance of the agency's software or equipment which could be used to access information or control systems without the provider taking any step that would contravene Part 13 of the *Telecommunications Act 1997*: o If the agency is given direct access to meta data or information in this way, the mechanism set out in 317ZH does not operate to require that the agency obtain an authorisation or warrant before accessing metadata or other information. This happens because the effective operation of 317ZH(1) depends upon the assumed application of Part 13 of the *Telecommunications Act 1997* to the information held by the provider (317ZH (2)(b)). However, Part 13 of the *Telecommunications Act 1997* (in particular Section 276) only applies a restriction on the 'use and disclosure' of certain information by the provider. 317ZH(1)says that a warrant or authorisation is required where the provider would have to make a use or disclosure that is contrary to its obligations in Part 13. (i.e. that it must be the provider making the disclosure and the act of disclosure by the provider must be one that requires a warrant or authorisation). Once an agency has software or equipment in the providers system it may be able access information without involving the provider: access to the information could be achieved without 'use or disclosure' by the provider. The access	• Include reference to *Telecommunications Act 1997* as new item (c). • Remove 317H(4) and (5). • Add to 317ZH(2) new subparagraphs (c) and (d) to read: o (c) assume that third party access, including virtual access or control of any software, equipment, component or system, would contravene Section 276; and (d) assume that third party access to or exfiltration of any information or documents from a designated communications provider would contravene Section 276. o delete "and" from the end of 317ZH(2) (a).

			could be obtained directly and independently by the agency. In this way, 317ZH as drafted appears to allow an agency to install software or equipment into a provider system and get direct access to metadata or information without obtaining a warrant or authorisation. o If the agency is given direct control of the provider's system by agency software or equipment the agency may be able to take steps that would in ordinary course be authorised by a warrant such as 'adding, copying, deleting or altering data in a computer' or 'any thing reasonably necessary to conceal the fact that anything has been done'. Part 13 of the *Telecommunications Act 1997* does not contemplate the possibility that a regulated party will not protect its systems from third party interference. As discussed in the point above the obligations expressed as obligations of the regulated party. Accordingly, if software or equipment installed by an agency enables the agency to take direct control of service provider systems without service provider involvement, the requirements expressed in 317ZH appear to operate in a manner that would allow the agency to exercise direct control without obtaining a warrant.	
20	317DA; 317P; 317Q; 317V: 317X	Judicial agreement to TAN and TCN (and variations)	• Fully support a warrant based-system with judicial oversight (i.e. warrants not to be issued by other persons such as a Justice of the Peace etc.)	• Agree with suggested Labor amendment as per motion. • Consider if the sections on 'Decision-making criteria' is the most appropriate place (alternative: sections that relate to the approval of the notice, e.g. 317TAAA).
21	317ZH	General limits on TAR, TAN, TCN	• The amendments included by the Government do not appear to be useful. Why has the Intelligence Services Act 2001 been deleted?	• Agree with suggested Labor amendment as per motion.
22	Throughout Act	TAN	• We suggest removing TANs from the legislation because: o The delineation between TAN and TCN is difficult and it appears that (without further amendments), due to the extensive scope of LATs, a TAN could be misused to request help that ought to be given under a TCN only. o The consultation requirements for TANs would require further improvement. o TANs are not afforded the right to an independent assessment and report when this would be required given the concerns above. • It would greatly reduce complexity.	• Remove TANs from the legislation.

3. Conclusion

The Associations look forward to continued engagement with the PJCIS, the Department of Home Affairs, and other relevant stakeholders on the mutual objective to protect Australians from crime, to enforce law and to enable the intelligence, interception and enforcement agencies to effectively do so in a rapidly evolving digital environment. However, these needs must also be balanced by supporting Industry innovation and the ability for Australian Industry to compete in a global market. Australian businesses and Government agencies also need to be able to access the most current cybersecurity and encryption technology to ensure their global competitiveness.

As highlighted in our submission, the Associations believe that the current Act requires further amendments to ensure that the legislation does not weaken existing cybersecurity structures, that it balances security and privacy considerations and minimises unintended consequences.

For any questions relating to this submission please contact