Thank you for the opportunity to provide feedback on the *Telecommunication and other Amendment (Assistance and Access) Bill 2018*.

AIIA makes this submission in addition to our joint submissions with Communications Alliance and the Australian Mobile Telecommunications Association (AMTA).

AIIA gives consent for this submission to be published.

Australian Information Industry Association

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 does this by providing a strong voice on policy priorities; creating a sense of community through events and education; enabling a dynamic network of collaboration and inspiration; and curating compelling content and relevant information.

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. We represent global brands including Apple, Adobe, Cisco, Deloitte, DXC, Gartner, Google, IBM, Infosys, KPMG, Lenovo, Microsoft and Oracle; international companies including Optus and Telstra; national companies including Ajilon, Data#3, Technology One, SMEs including Zen Enterprise and Silverstone Edge and start-ups such as OKRDY. While AIIA's members represent around two-thirds of the technology revenues in Australia, more than 90% of our members are SMEs.

Our national board represents the diversity of the digital economy. More detailed information about the AIIA is available on our web site: www.aiia.com.au

KEY AIIA Recommendations

The three key AIIA recommendations in relation to this Bill are as follows:

1. that AIIA members as well as other ICT industry representatives be engaged actively in further consultations on issues identified in this submission prior to the Bill being introduced into Parliament;
2. a regulatory impact assessment be published in relation to this Bill; and
3. an independent privacy impact assessment be undertaken in relation to proposed application of this Bill and privacy protection afforded under the Privacy Act 1988. The result of the assessment should be made available publicly.

AIIA observations and concerns

AIIA is a strong advocate for cybersecurity, data protection and the protection of privacy. The industry already provides law enforcement and intelligence agencies with assistance under the Data Retention

Regime, the Telecommunications Sector Security Reform and through the workings of interception legislation and assistance obligations under the *Telecommunications Act 1997*.

AIIA supports the continued efforts against the use of technologies including encryption being used by terrorists, child sex offenders, and organised criminals to conceal their illicit activities.

However, AIIA considers that the best way to achieve the outcomes proposed by the Exposure Draft is through collaboration between government and industry. In its current form the proposed Bill is broad, complex and ambiguous in many areas. It lacks clarity around what it is trying to achieve and many of the proposed new powers are ill-defined.

AIIA members' concerns are detailed below:

A. Lack of definitions will give rise to uncertainty in application and compliance with the legislation

The Exposure Draft suffers from a lack of definitional rigour. For example,

a) "Systemic weaknesses or vulnerabilities cannot be implemented or built into products or services". The definition of what is meant by "systemic weaknesses or vulnerabilities" is required. At what point does a measure that is introduced become "systemic"?

b) The Bill provides for a broad range of service providers – It might include telecommunication companies, internet service providers, email providers, social media platforms and a range of other "over-the-top" services. It also covers those who develop, supply or update software, and manufacture, supply, install or maintain data processing devices. Notices can be issued to a Designated Communications Provider's supply chain without their knowledge, or to equipment manufacturers that do not handle or have access to the required data. There is a concern that it is so broad as to effectively mean that the legislation can be applied in any context that an agency wishes. The definition of Designated Communication Provider, eligible activities' and 'listed acts or things' should be narrowed in consultation with providers.

B. Lack of transparency in Decision Making will not help to foster collaboration between industry and government in protecting Australians citizens and business against crime

a) In the case of technical assistance Notices, these can be issued by the head of ASIO or an interception agency or senior officials who have been delegated the authority in those agencies. Requirements in the Notices need to be reasonable and proportionate. AIIA members have concerns about the subjective nature of determining what is reasonable and proportionate nature and the technical capability of senior agency staff to make this assessment in a consistent manner. While the head or delegate is required to enter into a dialogue with the provider prior to the issuance of a Notice, the lack of specification/guidance on the minimum requirements of what constitutes a dialogue is of concerns to AIIA members. Therefore, AIIA members would like to see some minimum criteria/guidance as to what is reasonable and proportionate and clarity on what constitutes a dialogue between a delegate and provider in order to manage expectations from both side.

b) It is proposed that Notices will be issued based on the opinions of individuals at the agencies or in their chain of command. However, we note that Notices are not subject to administrative

review and there are only limited options to seek judicial relief for Notices that have been issued. We note that the UK Investigatory Powers Act introduced a secondary authorisation from a judicial officer to obtain a technical capability warrant as a result of consultations and AIIA members would like to see this adopted in the Australian Bill as well.

c) Limited scrutiny at a parliamentary level together with delegated decision making further undermine the transparency of the proposed system and introduce scope for abuse, duplication, inconsistency in application and lack of coordinating between agencies. Designated Communication Providers maybe subject to multiple warrants from multiple agencies if there is no centralised coordination through one agency. AIIA recommends that a system for coordinating agency requirements be developed in collaboration between all relevant agencies and industry.

d) "Notices must be revoked if requirements cease to be reasonable". It is unclear who is responsible for making this decision and against what criteria. Furthermore, it is unclear what action will be taken in relation to the information that has been collected up to the point that a decision is made. AIIA recommends elaboration on these points including what is test for reasonableness and how costs incurred by provider prior to the Notice being revoked will be calculated.

e) It will be difficult for the "cost negotiator "to have the necessary experience or knowledge to consider the full scope of terms and protections that a service provider may need to address to comply with a Notice. AIIA members are concerned that without industry involvement, the likelihood of costs being accurately calculated by a cost negotiator is unlikely and may lead to protracted discussions between government agencies and providers leaving providers out of pocket. This may have negative consequences for providers that are small businesses.

f) Where there is a disagreement between a provider and Government on the terms and conditions for compliance with a Notice, there is an option for an arbitrator to be appointed. The arbitrator will be appointed by Australian Communications Media Authority or the Attorney General, with the latter also having the power to issue Notices. AIIA members have concerns that the arbitrator will not be independent. AIIA recommends that the checks and balances are put in place to ensure the independence of the arbitrator.

C. Operational uncertainty and overreach will create uncertainty for industry

a) It is not clear in the Bill what requirements can or will be imposed beyond providing access to information at points where it is not encrypted. There is an extensive scope of acts and things that can be requested by the relevant agencies. AIIA members recommend that there be some published guidance on what can be requested and this guidance be updated from time to time in consultation with providers.

b) The full implication under the Exposure Draft of the issuing of Technical Assistance and Technical Capability Notices (Notices) is unclear. Issuing of Notices will require providers to find new ways to provide access to information and providers may not be able to comply with the Notice and still provide end to end encryption. What is not clear is whether "reasonable cost" to provider includes cost to the provider business for failure to provide end to end

encryption to its customers as a result of complying with a Notice or whether this will fall under exemptions of civil liability.

c) Technical Assistance and Technical Capability Notices may lead to technology vulnerabilities. The Bill includes a specific safeguard that a Technical Assistance or Technical Capability Notice cannot require a designated communications provider to implement or build a systemic weakness or a systemic vulnerability into a form of electronic protection. However, a service provider can still be required to (i) provide assistance or build capabilities that impact the security of the service provider's system, products or services in a non-systemic way, or (ii) to implement or build a systemic weakness or vulnerability into something other than "a form of electronic protection". AIIA members note that these latter requirements have the potential to compromise the quality of the service they provide to customers including government customers.

d) The scope of agency notices is limited to core functions. Core functions cover the spectrum from "protecting revenue" to "national security" and enforcement of criminal laws – in other words almost the entirety of government functions and responsibilities across a majority of government agencies. The draft Bill also in effect extends these "core functions" to any act or thing that is ancillary or incidental to a relevant objective of the agency. It is also assumed (but which is neither explicitly included or excluded in the Bill) that other government agencies can make requests through a designated interception agency thereby greatly expanding the scope of agency notices. AIIA recommends further discussions on the definition of core functions of an agency.

Overlap with existing legislation increases the compliance burden on industry

a) The Bill introduces side effects and ways to by-pass existing interception and data retention legislation. The explanatory document states that the powers in the Bill "cannot be used to impose data retention capability or interception capability obligations". However, the language in section 317ZH does not prevent a Notice from requiring a service provider that is not a carrier or carriage service provider from facilitating or installing a data retention or interception capability.

b) The enforcement of criminal laws in other countries may mean international requests for data will be funnelled through Australia as the "weakest-link" of our Five Eyes allies. This is because Australia has no enforceable human rights protections at the federal level. AIIA members are concerned on the flow on effect of this, that is, a high volume of Notices on providers. Complying with the notices may have a negative effect on these providers especially small businesses who are unlikely to dedicated resources to deal with such Notices.

c) Australian's trust in a range of digital technologies, service providers, and government may be eroded in an environment where service providers are directed to take actions directed by law enforcement and political officials.

Other issues

a) It is unclear whether a Regulatory Impact Statement will be published in relation to this Bill.

b) A privacy impact assessment has not been undertaken to understand how the proposed Bill will impact on privacy protection afforded Australian citizens under the Privacy Act 1988.

Kishwar Rahman
GM Policy and Advocacy
Australian Information and Industry Association

[redacted]