The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
PO Box 289
North Sydney NSW 2059
Australia
ABN 76 369 958 788

10 September 2018

National Security Policy Branch
Department of Home Affairs

Email: assistancebill.consultation@homeaffairs.gov.au

**COMMONWEALTH GOVERNMENT CONSULTATION ON THE ASSISTANCE AND ACCESS BILL 2018 (CTH)**

Dear Sir/Madam

Ai Group welcomes the opportunity to make this submission on the Assistance and Access Bill 2018 (Cth) (the Bill).

The future and increasingly the present of industry is the universal use of networked systems and the embedding of communications, digital and ICT in all processes and products. This Bill is therefore relevant and of potential concern to a wider range of businesses than may have been originally envisaged by the Government. In particular, this consultation is of intense interest to the many affected businesses represented by Ai Group, including those who offer cloud services, networked systems, telecommunications services and telecoms or IT hardware or other services. These include not just "communications businesses" and "IT businesses", but also a wide range of manufacturers and industrial solutions providers whose products and services are increasingly networked and digital.

An underlying industry concern with legislation of this type is whether it will create a loss of trust between businesses and their customers by compromising, or being seen to compromise, their privacy, data protection rights, security or safety.

Ultimately, the proposed changes in this Bill need to be effective and proportionate to the real needs of law enforcement and intelligence agencies in the digital world. The powers established and refined in the Bill should not be used as a default where alternative means may be available, and should be used only where the benefits to the community outweigh the costs – including the impact on trust and confidence in networked systems.

We support more collaborative approaches between Government and industry rather than resorting to regulation in the first instance. Where regulation is necessary, it is important that a holistic and balanced approach is taken to ensure public trust is not diminished and industry is not discouraged from operating and investing in Australia.

In absence of a more collaborative and holistic approach, the regime also runs the very serious risk that it will not be adaptable or flexible enough to tackle the risks that will emerge, as well as potentially creating unintended consequences. Cyber threats and tools to counter them are ever changing; risks and vulnerabilities will emerge even as past concerns are resolved. Traditional "command-and-control" regulatory frameworks will not be agile enough to meet this 21st century challenge.

Ai Group and our members would welcome the opportunity to work closely with the Government to improve this Bill.

**1. Consultation process**

Prior to public consultation, we understand that the Government may have undertaken preliminary consultation with a sample of technology and major telecommunications companies. While this is an improvement on processes such as the initial consultation stages of the Telecommunications Sector Security Reform (TSSR), this sample of companies does not reflect the wider range of industries captured by this Bill. For example, systems connected to the telecommunications network, supported by companies that supply or use the Internet of Things (IoT), Industrial IoT and Industry 4.0

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

technologies and solutions may be affected and do not appear to have been consulted prior to public consultation.

In the period since August when this consultation commenced, our discussions with members suggest very strongly that further and more structured consultation with industry is required. For a Bill that will likely have a material and wide impact on industry and the broader community, it is important that the consultation process is not rushed and adequately takes into account stakeholder feedback.

The current tight timeframe for the Bill does not allow for considered industry input at the level that would be most useful, especially considering the extensive volume of material under consultation. We would welcome the opportunity to work with the Government to bring together a range of industries who may be affected by this Bill for further consultation.

We also consider that a better process would involve extending the consultation process by adding an additional stage involving the publication of a revised Bill and Explanatory Memorandum and any other relevant materials for final review following further consultations on the present draft. This is in line with best practice consultation as conducted by the Productivity Commission for instance.

***Recommendation:***

- ***Conduct further structured industry consultation on the existing draft of the Bill; and***
- ***Publish a revised Bill and Explanatory Memorandum for final review by stakeholders.***

## 2. Preliminary industry views

Given the short timeframe for comment, we provide high level comments below for the Government's consideration.

We also note that the Communications Alliance and the Australian Mobile and Telecommunications Association have made a joint industry submission to the Government, which we broadly support.

### 2.1 Backdoors

We note that the Government does not intend for this Bill to deal with encryption or require the creation of "backdoors", which may be inferred under proposed section 317ZG. This refers to not requiring the designated communications provider to implement or build a systemic weakness or systemic vulnerability.

If we consider the hypothetical scenario where a suspected criminal user of a provider's hardware or services is investigated by a law enforcement agency, that agency could seek a Technical Capability Notice (TCN) for the provider to build a technical capability or functionality to facilitate access to data (for example, a one-off firmware update targeted at that suspect and no one else). The Government has argued a narrow definition, stating that a systemic weakness or systemic vulnerability does not arise when an individual is targeted and not the entire system.

However, we are of the view that introducing any type of technical capability or functionality to grant access to a user's hardware or services potentially creates a systemic weakness or vulnerability. This is because once developed it may be capable of extension to any and all users and could also create an opening for others to take advantage of new and existing weaknesses in the system. We discuss how this could be addressed below.

### 2.2 Broad definitions

We note that the proposed legislative obligations apply to any provider of communications services and devices in Australia, irrespective of where they base their corporation, services or manufacturing. The Bill refers to these as "designated communications providers", as defined under proposed section 317C. Proposed section 317E also specifies the listed acts or things which designated communications providers may be compelled by the Attorney General to do or provide. Both sections 317C and 317E are very broad ranging.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

We would be concerned if broadly and vaguely scoped legislation could compel companies to build security vulnerabilities into their products; this would affect *all* users of that product and result in weaker security for everyone. Section 317ZG attempts to allay this fear by specifying that a provider must not be compelled to implement or build a systemic weakness or vulnerability. However, the effect of this is ambiguous, particularly since listed acts or things are likely to be widely applicable for granting access to otherwise secure data.

***Recommendation: The definitions of "designated communications provider", "eligible activities" and "listed acts or things" should be narrowed based on consultation with the full range of affected stakeholders.***

### 2.3 Oversight of powers

We note that the Explanatory Document refers to oversight of powers which would be underpinned in the following areas: powers reserved to decision-makers; additional reporting requirements to provide transparency; inherent review by the courts; and arbitration for disputes on terms and conditions.

In this area, important improvements should be made to the Bill:

***Recommendations:***

- ***Requests should be coordinated through a central agency to minimise duplication. Relatedly, an authorised agency should be required to exhaust all other options (within that agency or via others) before making a request to a designated communications provider.***

- ***Amendments to section 34AAA of the Australian Security Intelligence Organisation Act 1979 (Cth) should be subject to the same limitation as that expressed in the proposed section 317ZG of the Telecommunications Act 1997 (Cth). That is, the warrant should not be used to render authentication or encryption ineffective.***

- ***Adopt an approach similar to the Investigatory Powers Act 2016 (UK), which introduced a secondary authorisation from a judicial officer to obtain a technical capability warrant as a result of consultations.***

### 2.4. Overseas considerations

According to the Explanatory Document (p. 8), "the Bill introduces new powers for agencies to secure assistance from the full range of companies in the communications supply chain both within and outside Australia". In practice, it may be difficult to enforce these obligations in certain overseas countries.

Related to this, it is unclear to what extent the Government has taken a holistic approach and adequately considered the practicality of creating domestic laws that may be ineffective, out of step and over-reaching with other relevant jurisdictions (as well as with other pieces of relevant domestic legislation). At worst, applying a stricter regime in Australia than overseas could impact Australia's digital capability and competitiveness, impeding network innovation, discouraging business presence in the Australian market, and leaving Australia behind. Additionally, this law could create a conflict for organisations operating in multiple jurisdictions if indeed it conflicts with data protection laws in operation in another country.

As previously stated in a joint industry submission on the TSSR,[1] it is imperative for Australia to leverage the important activities undertaken globally and to adopt, as much as possible, globally-

[1] Ai Group, Australian Information Industry Association (AIIA), Australian Mobile Telecommunications Association (AMTA), and Communications Alliance, Joint industry submission to the Parliamentary Joint Committee on Intelligence and Security on the Telecommunications and Other Legislation Amendment Bill 2016 (Telecommunications Sector Security Reform), 3 February 2017.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

consistent approaches. This will enable Australian agencies to work more effectively in concert with key foreign jurisdictions and ensure technology that is developed to address threats is consistent across the globe. We also urge the Government to establish effective cooperation arrangements between Australian and overseas agencies to obtain improved and timely threat information and cooperation and assistance to more effectively fight crime.

Also, by leveraging standards and best practices from other jurisdictions, Australia can utilise the techniques and tools that are available at economies of scale, rather than developing unique approaches that are likely to be considerably more expensive.

***Recommendation: The Government should consult closely with all relevant international jurisdictions to align with best practice.***

We look forward to working closely with the Government to address the above issues in the near future. Should you be interested in discussing our submission further, please contact our adviser Charles Hoang

Yours sincerely,

**Peter Burn**
**Head of Influence and Policy**

The Australian Industry Group
Level 2, 441 St Kilda Road
Melbourne VIC 3004
PO Box 7622
Melbourne VIC 3004
Australia
ABN 76 369 958 788

27 September 2018

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Email: TOLAbill@aph.gov.au

**INDUSTRY CONCERN ABOUT THE ASSISTANCE AND ACCESS BILL**

Dear Secretary

The Australian Industry Group (Ai Group) would like to inform the Parliamentary Joint Committee on Intelligence and Security (PJCIS) that we plan to make a further submission to the Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, and would like the opportunity to testify before the PJCIS, whether individually or as part of a group of like-minded industry representatives.

At this stage, we would like to express our concern about the Bill and the Government's inadequate response to widespread stakeholder feedback.

Our discussions with members since the draft Bill was released for comment in August suggest very strongly that further and more structured consultation with industry is required. For a Bill that will likely have a material and wide impact on industry and the broader community, it is important that the consultation process is not rushed and adequately takes into account stakeholder feedback. We understand these concerns are widely shared by other affected businesses and organisations.

Despite this, the Government decided to introduce the Bill to Parliament and refer it to the Parliamentary Joint Committee on Intelligence and Security on 20 September 2018, just 10 days after the close of submissions on an exposure draft. We made a submission raising significant concerns and understand a plethora of other submissions were made with similar concerns. The Government does not appear to have seriously considered or responded to the views of a broad range of stakeholders including industry and civil society groups.

As the Bill is currently drafted, it is relevant and of potential concern to a wider range of businesses than may have been originally envisaged by the Government. This includes not just "communications businesses" and "IT businesses", but also a wide range of manufacturers and industrial solutions providers whose products and services are increasingly networked and digital.

An underlying industry concern with legislation of this type is whether it will create a loss of trust between businesses and their customers by compromising, or being seen to compromise, their privacy, data protection rights, security or safety.

Ultimately, the proposed changes in this Bill need to be effective and proportionate to the real needs of law enforcement and intelligence agencies in the digital world. The powers established and refined in the Bill should not be used as a default where alternative means may be available and should be used only where the benefits to the community outweigh the costs – including the impact on trust and confidence in networked systems.

We support more collaborative approaches between government and industry rather than resorting to regulation in the first instance. Where regulation is necessary, it is important that a holistic and balanced approach is taken to ensure public trust is not diminished and industry is not discouraged from operating and investing in Australia.

In the absence of a more collaborative and holistic approach, the regime may not be adaptable or flexible enough to tackle emerging risks and may have unintended consequences. Cyber threats and tools to counter them are ever changing; risks and vulnerabilities will emerge even as past concerns are resolved. Traditional "command-and-control" regulatory frameworks will not be agile enough to meet this 21st century challenge.

Should the Committee accept our request to testify, our adviser Charles Hoang can arrange the details.

Yours sincerely,

**Innes Willox**
**Chief Executive**