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

13 September 2019

Dr James Renwick CSC SC
The Independent National Security Legislation Monitor
Email: INSLM@inslm.gov.au

Dear Dr Renwick

INSLM Review of the Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission to the Independent National Security Legislation Monitor (INSLM) review of the *Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018* (Cth) (TOLA Act).

We note that the Parliamentary Joint Committee on Intelligence and Security (PJCIS) has referred this review to the INSLM, and for the INSLM to specifically consider whether the TOLA Act achieves an appropriate balance, contains sufficient safeguards for protecting the rights of individuals, and remains proportionate and necessary.

Industry is increasingly characterised by the universal use of networked systems and the embedding of digital capabilities and communications in all processes and products. The TOLA Act is therefore relevant and of potential concern to a wider range of businesses than may have been originally envisaged by the Australian Government. 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. Some suggest the scope of the TOLA Act is cast so wide that it also extends to businesses and individuals who operate websites, and potentially to any business and person who uses the internet. Ubiquitous smartphones and connected devices in the workplace and at home mean the effects could be extensive.

Reinforcing the points we made in a joint submission with other industry associations to the INSLM, Ai Group would like to highlight the following key points:[1]

- **Support in principle:** We have a mutual objective with Government to protect Australians from crime such as terrorism, to enforce law and to enable the intelligence, interception and enforcement agencies to effectively do so in a rapidly evolving digital environment. We look forward to continued engagement with the PJCIS, the Department of Home Affairs, and other relevant stakeholders. Indeed, Ai Group works closely with Government and its agencies on improving Australia's cybersecurity. Protecting the security of communications and information between businesses and their customers is of fundamental importance.

- **Lack of proper consultation:** The Act itself and subsequent amendments (6 December 2018) were drafted with limited consultation and within very short timeframes. A very large number of businesses, civil liberties organisations, academia and other national and international stakeholders have voiced their concerns with the Act, including the amendments and continue to do so. In the lead up to Parliament making this law, Ai Group also urged for further consultation by Government to ensure that the potentially broad impacts of the legislation are tested by exposure to a cross-section of industry and the broader community. Ai Group was especially concerned that there was limited consultation with wider industry,

[1] The industry associations involved were the Ai Group, the Communications Alliance, the Australian Information Industry Association, the Australian Mobile Telecommunications Association, the Digital Industry Group Inc. and the Information Technology Professionals Association. Further details of the joint submission can be found in our Joint Submission to the PJCIS's *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Submission No. 23, July 2019), Link: https://www.aph.gov.au/DocumentStore.ashx?id=48c43087-0ff3-40fe-ba39-cb72713d3491&subId=668167.

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

given the broader scope of companies that could be captured under this legislation than may have been originally envisaged by Government.

- **Negative industry impact:** The above 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. This has already led to unintended consequences, including Australia's image overseas in relation to trust in Australian products.[2] This issue goes beyond a global misunderstanding of the workings of the legislation. The damage being done to Australian industry is due to technology buyers and investors around the world having listened to the strong body of international and Australian expert opinion on the risks that the legislation creates for the security of Australian-manufactured technology equipment and systems.

- **Urgent amendments required:** We consider substantial amendments are needed as soon as possible to clarify the TOLA Act and limit its impact in the areas of greatest risk. These are to ensure that the Act does not weaken existing cybersecurity structures, that it balances security and privacy considerations and minimises unintended consequences, particularly the ability of Australian businesses to compete.

More generally, an underlying concern is that the TOLA Act has the potential to weaken existing cybersecurity and privacy of all Australians. Cybersecurity threats remain a growing and evolving risk management issue for many businesses. The introduction of the TOLA Act creates an additional layer of risk, which may include impacting on the ability of Government and business to access international security and encryption products, making Australian businesses, Government agencies and the broader community vulnerable to cyberattack and data breaches. It is unclear how this will be monitored and addressed.

On the other hand, positive public initiatives such as AustCyber and the Australian Cyber Security Centre for promoting a cyber secure industry should be commended, despite being potentially undermined by the controversial issues with the TOLA Act. We have therefore been separately advocating with Government to review the 2016 revised National Cyber Security Strategy with input from all affected stakeholders, which has now commenced on 6 September.

In the meantime, Ai Group and our members would welcome the opportunity to work closely and meet with the INSLM to improve the TOLA Act.

Should the INSLM be interested in discussing our submission further, please contact our Digital Capability and Policy Lead Charles Hoang (02 9466 5462, charles.hoang@aigroup.com.au).

Yours sincerely,

Peter Burn
Head of Influence and Policy

[2] See Australian Strategic Policy Institute, "Perceptions survey: Industry views on the economic implications of the Assistance and Access Bill 2018" (December 2018), p. 3.