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

12 November 2020

Department of Home Affairs
Submitted via consultation website

Dear Sir/Madam

CRITICAL TECHNOLOGY SUPPLY CHAIN PRINCIPLES DISCUSSION PAPER

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission to the Department of Home Affairs (Home Affairs) on its draft Critical Technology Supply Chain Principles (Principles). Our members are businesses of all sizes and many sectors across Australia. As shown with COVID-19, many of these businesses are essential, contribute to our economy and form critical parts of supply chains and critical infrastructure.

1. General comments

Overall, we support Home Affairs's intention for its proposed Principles to remain voluntary and non-binding. And we support a security-by-design approach supported by principles (such as those proposed in the Discussion Paper), with the ultimate objective of protecting Australia's critical technology supply chains. We support measures to build trust and improve the security and resilience of our critical infrastructure and supply chains, with non-regulatory approaches as the default response before contemplating heavier forms of regulation. We believe this approach will create a flexible environment for all stakeholders to shape and implement best practices in a collaborative manner and encourage – rather than inhibit – innovation and productivity.

It is also important to be mindful that considering supply chain security and resilience for critical technology should not mean insulating Australia from international engagement and competition. For example, one of the major intrinsic benefits of advanced manufacturing is the increased capacity to export to global markets and integrate with global value and supply chains. In this area, Industry 4.0 technologies and digitalisation, supported by trusted partners (local and global), can play a role in building resilience in our global network.

We note, however, that limited time has been allocated to consult on this Discussion Paper including its proposed Principles. The Discussion Paper indicates that the Government may decide that further work is required after its development as part of its plan to review the Principles after 12 months of voluntary implementation. If that is the case, it will therefore be important to recognise other various initiatives in place or under way to ensure proper consideration has been given to these other activities. We would therefore encourage Home Affairs to properly consider these other initiatives and consult further with stakeholders should relevant matters arise in the course of developing these Principles.

We welcome being included as part of further consultations and bringing in relevant members covering a wide range of sectors that may be interested in participating. We would also appreciate the opportunity to work closely with Home Affairs as the consultation progresses.

In the meantime, we would like to provide preliminary views relating to other initiatives where we have made submissions that may be equally relevant to this consultation. As further consultation is undertaken, there may be additional matters raised.

2. Relevant government consultations and other initiatives

We welcome the Government's acknowledgement of the various initiatives (including several references[1] and non-exhaustive list in Annex B of the Discussion Paper) and intention that the Principles will complement other existing Government efforts to ensure the resilience of supply chains. The Discussion Paper notes that this will be complemented by Home Affairs and the Department of Industry, Science, Energy and Resources (DISER) both reviewing the feedback received.

Nevertheless, it is important to also recognise that several consultations and initiatives are still under development, including issues that require clarification and development, and may be directly related to the Principles. Therefore, it is important to not only consider the complementary role in which these Principles may serve, but also appreciate how they will interact with these other activities. By doing so, it will likely assist potential users to better understand the utility of these Principles together with these other activities from a holistic perspective.

Further, some of these issues are being managed by other Government agencies and bodies, and it will be important for Home Affairs and DISER to properly coordinate and understand the scope of these issues. Otherwise, there is a risk of overlapping and conflicting issues. Therefore, further intergovernmental engagement beyond Home Affairs and DISER may also be required as a result of these broader considerations, such as Treasury, DFAT, Prime Minister's Digital Technology Taskforce, and the Department of Infrastructure, Transport, Regional Development and Communications (DITRDC).

For example, below is a non-exhaustive list of different government consultations and initiatives that we consider are relevant for consideration in relation to the proposed Principles. Where possible, we have also referenced our previous submissions covering similar issues that may be relevant to the questions raised in this Discussion Paper:

- The ACCC's Digital Platforms Inquiry – Government's response to this Inquiry includes policy reforms in the area of privacy and data regulation.[2] Following this Inquiry, the Attorney General's Department has now commenced its review of the Privacy Act.[3]

- DITRDC's consultation on a new Online Safety Act – online safety proposals in this consultation may be relevant to the Principles under consideration.[4]

- Home Affairs's *Voluntary Code of Practice: Securing the Internet of Things for Consumers* – a range of matters with respect to the proposed Code of Practice including principles that may be applicable to the Principles discussed in this consultation.[5]

- Home Affairs's consultation on *Protecting Critical Infrastructure and Systems of National Significance* – Home Affairs considers that its Principles will complement the critical infrastructure security reforms. Our submission raises several issues including details that currently remain unclear and require further consultation such as the nature of the reforms, scope, definitions, measures and cost-benefit impact.[6] For example, this consultation may

[1] Some references mentioned in the Discussion Paper includes: ACSC's guidance on cyber supply chain risk management; Business.gov.au guide on business risks; Australia's 2020 Cyber Security Strategy; Voluntary Code of Practice: Securing the Internet of Things for Consumers; ACSC's Strategies to Mitigate Cyber Security Incidents – Mitigation Details; Black economy – increasing the integrity of government procurement: Procurement connected policy guidelines.
[2] Ai Group submission to Treasury (September 2019), Link: https://cdn.aigroup.com.au/Submissions/Technology/AiGroup_submission_Digital_Platforms_Inquiry.pdf.
[3] Commonwealth Attorney-General, *Review of the Privacy Act 1988*, Link: https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988.
[4] Ai Group submission to Commonwealth Department of Infrastructure, Transport, Regional Development & Communications, *Consultation on a new Online Safety Act* (February 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/New_Online_Safety_Act_Proposals_21Feb_2020.pdf.
[5] Ai Group submission to Home Affairs (February 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Securing_IoT_for_Consumers_Voluntary_Code_of_Practice_Feb_2020.pdf.
[6] Ai Group submission to Home Affairs (September 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Dept_Home_Affairs_Critical_Infrastructure_Security_Reforms_Sept2020.pdf.

also require clarifying the scope and definitions and providing guidance, such as on: "critical" and "supply chain" to assist in determining risk management obligations; and how responsibility is applied in the supply chain and what is within an entity's control to its best endeavours.

- Treasury consultation on *Major reforms to the Foreign Investment Review Framework* – we consider that there are potential interactions between Home Affairs's critical infrastructure security reforms and Treasury's reforms. In particular, Treasury's proposed changes to the *Foreign Acquisitions and Takeovers Act 1975* (Cth) (FATA) would subject any business responsible for, or with a significant stake in, critical infrastructure covered by the *Security of Critical Infrastructure Act 2018* (Cth) (SCIA) to substantial new obligations and powers under the FATA. Thus decisions about the scope of the SCIA will have larger implications that need to be fully considered in regulatory impact analysis.[7]

- Treasury's consultation on its *Inquiry into Future Directions for the Consumer Data Right* – relevant to the Principles, we raised several interrelated issues including on privacy, data protection and cyber security.[8]

- Treasury's consultation on *Improving the Effectiveness of the Consumer Product Safety System* – insofar as the Principles relate to the consumer, supply chain security may also fall under the scope of Treasury's consultation if it leads to consumer safety issues.[9]

- Parliamentary Joint Committee on Intelligence and Security (PJCIS) and Independent National Security Legislation Monitor (INSLM) reviews relating to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA Act) – there are concerns about the potential negative impact of this Act on cyber security and privacy of products and services.[10] We have recently made a supplementary submission supporting the INSLM's recommendations.[11]

- The PJCIS review into the effectiveness of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 – we consider this Bill is interrelated with the TOLA Act review.[12]

- The Standing Committee on Communications and the Arts Inquiry into 5G in Australia – while cyber security has been excluded from this Inquiry, there are interrelated considerations with respect to the operation of 5G and IoT.[13]

---

[7] Ai Group submission to Treasury (September 2020), Link: https://cdn.aigroup.com.au/Submissions/Trade_and_Export/Submission_FATA_reforms_September_2020.pdf.
[8] Ai Group submission to Treasury (June 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Treasury_CDR_Inquiry_5Jun_2020.pdf.
[9] Commonwealth Treasury, *Improving the Effectiveness of the Consumer Product Safety System*, Link: https://consult.treasury.gov.au/market-and-competition-policy-division-internal/main-consultation.
[10] Joint submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS), *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act)* (Submission No. 23, July 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions; Joint submission to the Independent National Security Legislation Monitor (INSLM), *Review of the TOLA Act* (Submission No. 15, September 2019), Link: https://www.inslm.gov.au/submissions/tola; Ai Group submission to the INSLM, *Review of the TOLA Act* (Submission No. 12, September 2019), Link: https://www.inslm.gov.au/submissions/tola; Australian Strategic Policy Institute (ASPI), *Perceptions survey: Industry views on the economic implications of the Assistance and Access Bill 2018* (December 2018), p. 3.
[11] Ai Group supplementary submission to PJCIS (Submission No. 23.1, July 2020), Link: https://www.aph.gov.au/DocumentStore.ashx?id=d40979d1-6ce6-4460-a6d5-bd903f757cb8&subId=668167.
[12] Ai Group submission to PJCIS (Submission No. 32, May 2020), Link: https://www.aph.gov.au/DocumentStore.ashx?id=f73c608e-f21d-42a0-972d-56aebbcd7d57&subId=682819.
[13] Ai Group submission to Standing Committee on Communications and the Arts, *Inquiry into 5G in Australia* (Submission No. 356, November 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Communications/5G/Submissions.

- The Australian Human Rights Commission's (AHRC) consultation into Human Rights and Technology – as the title suggests, the AHRC have been exploring the impact of emerging technologies on human rights.[14]

- DISER's AI initiatives such as the AI Ethics Framework including principles, and its recently commenced consultation on an AI Action Plan.[15]

- The Ambassador Cyber Affairs and Critical Technology Engagement within DFAT has been consulting on Australia's International Cyber and Critical Technology Engagement Strategy, which will potentially be relevant to Home Affairs's consultation.[16]

- With respect to standards, there already exists standards (especially international) and initiatives to support industry standards relevant to critical infrastructure and systems that may address or respond to the Principles in Home Affairs's Discussion Paper. For instance, Standards Australia's AI Standards Roadmap includes references to standards.[17] Also, Ai Group is involved in a partnership with the NSW Government, Standards Australia, AustCyber and other key industry stakeholders to harmonise cyber security standards across several key sectors. There is an opportunity for the scope of this work to be expanded to other sectors.

If you would like clarification about this submission, please do not hesitate to contact me or our Lead Adviser – Industry Development and Defence Industry Policy, Charles Hoang (02 9466 5462, charles.hoang@aigroup.com.au).

Yours sincerely,

Louise McGrath
Head of Industry Development and Policy

[14] Ai Group submission to AHRC, *Discussion Paper on Human Rights and Technology*, Link: https://cdn.aigroup.com.au/Submissions/Technology/AHRC_Human_Rights_and_Technology_Discussion_Paper_26Mar_2020.pdf.
[15] DISER, *AI Action Plan*, Link: https://www.industry.gov.au/news-media/australias-ai-action-plan-have-your-say.
[16] DFAT, *International Cyber and Critical Technology Engagement Strategy*, Link: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/public-consultation-international-cyber-and-critical-technology-engagement-strategy.
[17] Standards Australia, *Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard* (March 2020), Link: https://www.standards.org.au/news/standards-australia-sets-priorities-for-artificial-intelligence.