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

26 November 2020

Department of Home Affairs
Email: ci.reforms@homeaffairs.gov.au

Dear Sir/Madam

PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE – EXPOSURE DRAFT BILL

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission to the Department of Home Affairs (Home Affairs) on its consultation on its Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Exposure Draft Bill), and accompanying documents including the Draft Explanatory Document.

1. Consultation process

We note that this consultation follows the initial Consultation Paper stage as part of the *Protecting Critical Infrastructure and Systems of National Significance* (PCISNS) reforms. Given the potential significant and wide impact of these reforms, it is imperative that extensive consultation is undertaken, including on an Exposure Draft Bill. We therefore support this next stage of consultation for these reforms.

While we appreciate the opportunity to comment on the Exposure Draft Bill, we note that this is the first real opportunity to comment on the detail of a technically complex and detailed piece of proposed legislation. Upon reviewing the associated documents, we consider that it raises more questions for industry.

As a result, we strongly consider that additional time is needed for deeper consultation on the Exposure Draft Bill, consideration of legitimate comments arising from this consultation (as demonstrated by the many published submissions received by Home Affairs at its initial consultation stage), and responsive amendments to the Exposure Draft Bill. The timeframe allocated for consultation and review on this Bill is relatively tight to enable sufficient scrutiny. There are also concurrent and potentially interrelated consultations underway by other Government Departments, which would need to be taken into proper account.

To provide an analogy, the Telecommunications Sector Security Reforms (TSSR) was developed for the telecommunications industry as part of the critical infrastructure security regime. This took several years of negotiation and collaboration between Government and industry before a more workable version was implemented. With respect to the PCISNS reforms, we expect that each affected sector receives similar levels of engagement with Government to ensure a genuinely collaborative and mutual outcome. And as noted in the Draft Explanatory Document, the TSSR is also currently under review by the Parliamentary Joint Committee on Intelligence and Security (PJCIS), as well as a range of other reforms and initiatives underway that are interrelated to the PCISNS reforms. It is therefore important that relevant matters arising from these other reforms and initiatives, as well as existing arrangements, are appropriately considered.

To date, we have welcomed the consultative approach that Home Affairs has undertaken in holding virtual town halls and industry specific workshops. We encourage that this level of stakeholder engagement continues for the remainder of the consultation process.

We would also welcome our continued inclusion in further consultations, along with relevant members covering a wide range of sectors that may be captured by these reforms, and the opportunity to work closely with the Department of Home Affairs as the consultation progresses.

Should the Exposure Draft Bill reach the stage for Parliamentary consideration, we strongly recommend that the PJCIS and Independent National Security Legislation Monitor (INSLM) be included as part of the review of the Bill. However, at this stage, we suggest that it would be premature for the various reasons summarised above.

In the meantime, we would like to provide preliminary views, particularly on the Exposure Draft Bill and Draft Explanatory Document. As further consultation is undertaken, there may be additional matters raised.

Recommendation: Government allocate additional time for deeper consultation on the Exposure Draft Bill, consideration of legitimate comments arising from this consultation, and responsive amendments to the Exposure Draft Bill.

2. Regulatory Impact Statement (RIS)

The Draft Explanatory Document indicates that a qualitative RIS has been undertaken on the potential costs and benefits of the proposed reforms. It proposes that a more detailed RIS with quantitative cost-benefit assessment with respect to the Positive Security Obligation component will be undertaken when sector-specific rules are being developed, which will not occur until after the legislation is passed. It also indicates that a quantitative cost-benefit assessment with respect to the Enhanced Cyber Security Obligations, expansion of the critical infrastructure assets register, and mandatory cyber incident reporting will be provided upon commencement of the legislation. This infers that the detail of the requirements for each identified sector and their real cost impacts are currently unknown and will not be known until as late as the sector-specific rules are developed.

Where proposed legislation establishes a broad framework for future regulation, it would not be reasonable to expect the full ramifications of all future regulations to be assessed upfront. However, it is very reasonable to expect that the Government have a sufficiently specific idea of the initial regulatory steps (especially sector-specific rules) it wishes to take to enable these to be assessed alongside the enabling legislation.

Further, we are extremely uncomfortable with proposed reforms that have not been subject to a proper cost-benefit assessment, especially given reforms that have a significant wide impact across many sectors. We do not consider this to be consistent with best regulatory practice, and firmly oppose reforms that have not undertaken sufficient assessment including cost-benefit. It also creates uncertainty for industry regarding whether sector-specific rules will be developed, especially in a future scenario where a future quantitative cost-benefit assessment determines that there are no or limited net benefits.

Providing meaningful comments on the regulatory cost impact will also require further detail on developed options. As one member previously commented, it is impossible to estimate costs of such measures without the detail.

As part of a quantitative cost-benefit assessment, we consider the following should be taken into account:

- Government should factor in transitional assistance for companies to meet with new forms of compliance. For example, businesses may need to increase or upskill personnel capability to help them properly meet new regulatory obligations.

- Options should be assessed including: the current proposal; no policy change; and non-regulatory approaches to pursuing the benefits sought.

- The impact of these reforms on other Government initiatives (including public funding related) that are designed to help boost industry capability, investment and competitiveness. If the reforms result in a negative impact on the objectives and benefits of other publicly funded industry initiatives, this will need to be publicly accounted for. This also includes broader initiatives such as the Government's deregulation/red tape reduction policy and COVID-19 economic recovery agendas.

- While the Government's stated intention of these reforms are not to duplicate existing regulations, the RIS should factor in the cost of compliance of associated regimes (as well as existing arrangements) e.g. Notifiable Data Beaches (NDB) Scheme, Consumer Data Right

(CDR) and European Union General Data Protection Regulation (EU GDPR). This assessment will enable for proper consideration of the cumulative regulatory impact of multiple forms of regulation that may be interrelated or overlapping through these reforms.

- A Privacy Impact Assessment should also be undertaken as part of the RIS. For example, there could be associated privacy risks that may arise from Government intervention under these reforms that needs to be properly accounted for.

- Cost impact of risks associated with market intervention and regulatory uncertainty e.g. unintended consequences arising from direct government action (i.e. Government Assistance measures) and impact on company investment risk credit rating of entities subject to the new laws that may be perceived to be overly intrusive.

Recommendation: Government undertake a proper quantitative cost-benefit assessment for the proposed reforms prior to making legislation.

3. Scope of the Exposure Draft Bill

We appreciate that Home Affairs has consulted with representatives across the 11 critical infrastructure sectors that it has identified to be subject to the Exposure Draft Bill, and that the Draft Explanatory Document provides further clarification on definitions relating to each sector, critical asset, critical system, and responsible entity.

Our previous submission highlighted areas of uncertainty with respect to the proposed reforms. These related to the need for clarification on the details including on the nature of the reforms, scope, definitions, measures and cost-benefit impact. We note that the Exposure Draft Bill and Draft Explanatory Document provides further detail, however we consider that further clarification is still required.

For instance:

- Need for further clarity on definitions or guidance relating to the scope including “critical” and “supply chain”.

- To help define the scope of risk management obligations, there needs to be proper consideration on the extent of entity responsibility based on what is within their control. For example, how far will the scope of responsibility of an entity flow down the supply chain? There should also be flexibility for those along the supply chain to have their own processes in place to determine their critical assets. A best endeavours approach could be considered. Otherwise, imposing obligations on an entity to manage risks beyond their control will likely fail and impose compliance costs that will not achieve the desired objectives.

- There remains a potential concern as to how the reforms might apply to companies that have diversified portfolios and operate, service or supply assets to a range of sectors identified under this Exposure Draft Bill e.g. suppliers, manufacturers and “data storage or processing” sector. There is also a potentially higher regulatory burden created for SMEs and those not currently subject to critical infrastructure security legislation.

- The definition of “data and the cloud” appears to have been substituted with “data storage or processing”. While there is some clarification to this definition, it is still vague as many businesses may have data storage or processing, as part of their business models.

- The Draft Explanatory Document states that “This framework will apply to owners and operators of critical infrastructure regardless of ownership arrangements. This creates an even playing field for owners and operators of critical infrastructure and maintains Australia’s existing open investment settings, ensuring that businesses who apply security measures are not at a commercial disadvantage”. Notwithstanding this, the Government’s currently 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 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 a regulatory impact analysis.

Given the breadth and detail in the Exposure Draft Bill and Draft Explanatory Document, there will likely be other aspects and details within these documents that will require further scrutiny. The above comments are only preliminary examples. We appreciate that Home Affairs has hosted Town Hall virtual events, which provide an overview of the Exposure Draft Bill. However, we suggest that it might be beneficial if there was an opportunity for Home Affairs to walk through in detail with stakeholders on its proposed reforms, which may require several sessions to cover each component.

Recommendation: Home Affairs host a detailed walk-through with stakeholders on its proposed reforms, which may require several sessions to cover each component.

4. Positive Security Obligations (PSO)

4.1 Support for the intent

We welcome the Government's acknowledgement in the Draft Explanatory Document of the importance of partnering with industry as a foundation of a PSO and to co-design sector-specific requirements. If co-designed well, it can lead to positive outcomes such as: improving industry security posture; providing organisations with a risk management program to help protect their businesses and customers; providing better ways to identify and share security threats; avoiding duplicating existing regulatory approaches; applying a principles-based and proportionate approach; and minimising regulatory burden.

To this end, we support in principle the Government's intent for the PSO, which is to "embed preparation, prevention and mitigation activities into the business as usual operating of critical infrastructure assets, ensuring that the resilience of essential services is strengthened", and "provide greater situational awareness of threats to critical infrastructure assets". However, we may have alternative views on how it could be implemented.

4.2 Existing arrangements and gap analysis

The Government proposes to create the following obligations (PSO) for identified businesses:

- adopting and maintaining an all-hazards critical infrastructure risk management program;
- mandatorily report serious cyber security incidents to the Australian Signals Directorate (ASD and more specifically Australian Cyber Security Centre (ACSC)); and
- where required, providing ownership and operational information to the Register of Critical Infrastructure Assets.

Further discussion is needed on whether the PSO should be addressed via new regulation or legislation attached with civil penalties for non-compliance as proposed in this Bill, or whether the same objectives could be achieved through other means; for instance, by referring businesses to existing best practices such as recognised existing obligations and industry standards (especially international). It is not clear whether a proper assessment has been undertaken for each identified sector to determine whether these already exist to avoid the necessity of creating a PSO through legislation and duplicating existing obligations.

Existing industry standards (especially international) relevant to critical infrastructure and systems may address or respond to the concerns underlying Home Affairs's proposed reforms. For instance, 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.

And for businesses that operate across sectors such as cloud service providers, it may be difficult to consider whether and which proposed principles-based outcomes and proposed measures should apply to them, without first understanding the various security requirements for each specific sector that they service. To help resolve this, a possible solution could be to undertake a thorough gap analysis and assessment of the proposed obligations against existing obligations across the various sectors in which these businesses operate. Once these are clarified for the various sectors, further consideration could be given to businesses that operate across sectors such as cloud service providers. And if it were to be deemed that a regulator is required to be appointed, the regulator will

need to have the sufficient technical expertise to understand the complexity and nuances of cloud services, and the ongoing innovation and technology development in this space.

If a gap analysis and assessment of requirements for each specific sector were to be undertaken, we consider that further consultation will be required with relevant stakeholders. For instance, this may include: assessment of the level of maturity of practices; access to required standards and competencies to ensure vulnerabilities are identified, understood and risk controls put in place; readiness to be regulated; expected baseline competencies; and access to supported competencies training.

With respect to non-regulatory approaches, the value of education, communication and engagement activities should also not be underestimated, especially in building trust and facilitating genuine collaboration between governments and industry. This is acknowledged in the Draft Explanatory Document, noting that a refreshed Critical Infrastructure Resilience Strategy to incorporate these elements will help to "improve our collective understanding of risk within and across sectors".

Recommendation: At this stage, with respect to the PSO, we suggest that it would be premature to proceed with legislation without fully understanding the existing sector-specific arrangements for the reasons outlined above. Further engagement with industry will be required to progress discussions about the PSO.

4.3 Mutual obligations

Setting aside issues concerning existing arrangements for the moment, there appears to be a need to clarify mutual obligations between the ASD and entity. With respect to the proposed PSO requirement for an entity to mandatorily report serious cyber security incidents to the ASD, the Draft Explanatory Document suggests that this "will support the development of an aggregated threat picture and comprehensive understanding of cyber security risks to critical infrastructure in a way that is mutually beneficial to Government and industry. This will better inform both proactive and reactive cyber response options – ranging from providing immediate assistance to industry to working with industry to uplift broader security standards".

However, it is not clear if the intention of this PSO is reflected in legislation. If such a reporting obligation were to be required of an entity, it would be helpful to understand how the ASD will assist the entity following the provision of the entity's report. This would help to establish a genuine bilateral relationship of trust between the ASD and reporting entity.

A similar mutual understanding should also apply to the other proposed PSOs (as well as Enhanced Cyber Security Obligations discussed below) where the entity provides information with an understanding that the ASD will provide it with assistance. For example, how will the ASD assist the entity in uplifting its risk management program, or advise the entity of its security risk considerations having regard to its ownership and operational information?

Recommendation: A mutual obligation be created for the ASD to assist the entity if the entity is obligated to provide the ASD with requested information.

4.4 Unintended consequences

Generally, it is important to be mindful of the unintended consequences created by attaching civil penalty provisions for non-compliance on newly created obligations. We would also be cautious against creating regulation if its intent is to encourage collaboration. Regulation attached with civil penalties for non-compliance creates an adversarial framework, which would not seem propitious for collaboration.

For example, for the purposes of reporting on critical cyber security incidents, the Draft Explanatory Document states that the definition of such incidents is not defined as its significance may vary between assets. This would be left to the judgement of the entity with specific guidance from the Critical Infrastructure Centre. However, given the potential civil penalties attached to not reporting, there is a risk that some entities may decide to report an incident irrespective of its magnitude of seriousness or criticality to avoid any doubt. Such a scenario would be averse to the intention of this reporting obligation. This leads to regulatory burden on businesses to make more frequent reports (irrespective of the PSO's intent) and an administrative burden on the ASD to handle an increased volume of reports.

Recommendation: The purpose behind the proposed new legislative provisions including civil penalty provisions be reviewed, and other options be considered.

5. Enhanced Cyber Security Obligations (ECSO)

The Draft Explanatory Document notes that stakeholders supported for greater threat sharing and partnerships with Government, and considers that this will be enabled through the ECSO.

In principle, we support the concepts under the ECSO relating to incident response planning, cyber security exercise undertaking and vulnerability assessment undertaking. These activities help to build cyber security resilience and preparedness.

On the one hand, the Draft Explanatory Document expresses the Government's intention to "continue to build on the strong voluntary engagement and cooperation with critical infrastructure entities that has underpinned the success of the relationship to date". However, it suggests that "there may be instances where entities are unwilling or unable to voluntarily cooperate and the Enhanced Cyber Security Obligations are necessary". To reinforce this point, these obligations are attached with civil penalties for non-compliance.

Again, like the PSO, further discussion is needed on whether the ECSO should be addressed via new regulation or legislation, attached with civil penalties for non-compliance as proposed in this Bill, or whether the same objectives could be achieved through other means as discussed above with respect to the PSO. We consider similar concerns raised above about the PSO could also be extended to the ECSO.

For example, the Draft Explanatory Document notes that there already exists a non-regulatory risk management framework and obligation under the Defence Industry Security Program (DISP) managed by Defence in partnership with industry. While the Draft Explanatory Document appears to deem that the existing Defence security mechanisms under the DISP are appropriate insofar as it relates to the PSO, the Draft Explanatory Document suggests that the ECSO (if any critical defence assets are designated as systems of national significance) and Government Assistance measures will still apply for the defence sector. It is not altogether clear of the rationale for this.

The ECSO also includes an obligation where the Home Affairs Secretary may require an entity to provide system information that is intended to support the Government's ability to build near real time threat picture, share actionable and anonymised information back to industry, and target threats and vulnerabilities of greatest consequence to the nation. To implement this, an option in the ECSO proposal is that the Home Affairs Secretary could require an entity to install and maintain a specific computer program, within its system. As with the other proposed obligations, there is a civil penalty attached for non-compliance. While we support in principle information threat sharing with Government, there is a risk that this particular requirement may be regarded to be an overreach of Government powers and risk of (or perceived to be at risk of) abuse. Without appropriate safeguards and regulatory oversight, we can see similar issues and concerns that arose with the *Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018* (Cth) (TOLA Act) being repeated in this ECSO proposal. In this regard, we discuss further below about the importance of implementing appropriate regulatory oversight and safeguards.

Recommendation: At this stage, for similar reasons as the PSO, we suggest that it would be premature to proceed with legislation relating to the ECSO. Further engagement with industry will be required to progress discussions about the ECSO.

6. Government Assistance measures

The Draft Explanatory Document refers to its proposed Government Assistance measures as a last resort response to serious cyber security incidents to protect critical infrastructure sector assets during or following a significant attack. These authorised actions are categorised as information gathering directions, action directions and intervention requests.

In principle, we support Government's role in assisting in protecting our critical infrastructure. We appreciate the hypothetical scenarios provided in the Draft Explanatory Document to assist in clarifying by way of examples of when, where and how Government could undertake Government Assistance.

However, there will still likely be issues that require further clarification relating to the scope of Government Assistance measures and the process for authorising these measures. For instance, we seek further clarification on the following:

- The Draft Explanatory Document attempts to define the circumstances when these last resort powers can be used by meeting a set of criteria. One of these factors refers to "a material risk that the incident has seriously prejudiced, is seriously prejudicing, or is likely to seriously prejudice …". However, the terms "material risk" and "seriously prejudiced" appear to be undefined.

- Depending on the Ministerial authorised actions, the Minister has to be satisfied that certain conditions are met (e.g. in terms of practicality and effectiveness, reasonableness, proportionality, technical feasibility etc). The Draft Explanatory Document provides examples of how this could be interpreted. However, it is not clear of the decision-making process including appropriate expertise that the Minister has access to make that determination.

- With respect to action directions, the Draft Explanatory Document notes that "it is not possible to accurately foresee the many ways a system may be compromised or the actions that would be required to respond to the incident. Therefore, the Minister for Home Affairs' power to authorise the giving of a direction for the entity to do, or refrain from doing, a specified act or thing is left intentionally broad". However, this creates uncertainty for a direction that should be triggered in very limited circumstances (i.e. emergency) and therefore not be broad.

- The required capability of an authorised agency to provide Government Assistance on certain critical infrastructure. In the Exposure Draft Bill, the authorised agency is defined as the ASD.

- The liability of an authorised agency for negative unintended consequences arising from a Government Assistance, and redress for the impacted entity. For example, the authorised agency may be granted immunity from liability if it acted in good faith, despite potential negative unintended consequences that could have a material impact on the entity, its customers and wider community. As noted previously, this infers that there is a recognition that risk of errors that could arise and Government may be seeking to limit its own risks of liability. However, this leaves businesses exposed without equitable remedy; businesses will therefore need to disclose that risk to their shareholders and stakeholders, potentially suffering consequences such as increased cost of capital as shareholders perceive such risk, or relocation of investment overseas. This will need to be included as part of any cost-benefit assessment (as noted above).

As with the other components of these proposed reforms, there will likely be other aspects and details with respect to these last resort powers that will require further scrutiny, and the above comments are only preliminary examples.

Recommendation: At this stage, for similar reasons as other aspects of the proposed reforms, we suggest that it would be premature to proceed with legislation relating to the Government Assistance measures. Further engagement with industry will be required to progress discussions about this.

7. Safeguards and regulatory oversight

A significant concern that we have in relation to the Government's last resort powers is that the Draft Explanatory Document proposes to exempt authorisations made under these powers from being subject to judicial review. Some reasons provided are that they relate to national security considerations where sensitive information is involved and may be publicly disseminated through judicial proceedings, and the delays caused by judicial proceedings would not be suitable for emergency circumstances. Instead, it suggests that there are other safeguards and limitations that would be introduced to ensure Ministerial decisions only occur in exceptional circumstances and when it is in the national interest.

While we understand this rationale, we do not consider that the Government offers a satisfactory level of assurance to industry. There should be consideration of other options for providing adequate independent oversight. For example, similar considerations were given during the TOLA Act Review by the INSLM in consultation with a wide range of stakeholders. We endorse the INSLM's recommendations to the TOLA Act, especially in relation to improving independent oversight, and

suggest that it could also be a relevant approach for consideration in these reforms. The INSLM's recommended approach provides a more proportionate and balanced approach, enabling for the protection of our national security, while providing appropriate safeguards to protect the cyber security and privacy of businesses and the wider community.

Further, the INSLM and PJCIS should be empowered to review the effectiveness and proportionality of the legislation (say 12 months after commencing the legislation) and, as required, subsequent reviews of the legislation.

In addition to the last resort powers, we suggest that similar safeguards and regulatory oversight apply to other aspects of the proposed reforms where new Government (including Ministerial) powers are created; for example, with respect to the PSO and ECSO, as these obligations also act as a form of direct market intervention.

Recommendations:

- **Consideration be given to alternative options for independent oversight of new Government powers, such as the INSLM's recommended independent oversight approach for the TOLA Act.**

- **The PJCIS and INSLM be empowered to review the effectiveness and proportionality of the legislation and, as required, subsequent reviews of legislation.**

8. Concurrent and interrelated consultations and initiatives

We consider that there are various government consultations and initiatives that are relevant for consideration in relation to these reforms, with some already mentioned in our submission. We note that some of these interrelated consultations are occurring concurrently with similar tight deadlines, particularly towards the end of the year (e.g. AGD's Review of the Privacy Act, and DISER's consultation on its AI Action Plan). In terms of process, we recommend that better coordination should be undertaken by Home Affairs and other relevant Government agencies to enable for proper consultation for both this consultation and others underway.

Below is a non-exhaustive list. Where possible, we have also referenced our previous submissions covering similar issues that may be relevant to these reforms:

- The ACCC's *Digital Platforms Inquiry* – Government's response to this Inquiry includes policy reforms in the area of privacy and data regulation.[1] Following this Inquiry, the Attorney General's Department has now commenced its *Review of the Privacy Act*.[2]

- DITRDC's consultation on a new *Online Safety Act* – online safety proposals in this consultation may be relevant to these reforms.[3]

- 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 these reforms.[4]

[1] Ai Group submission to Treasury (September 2019), Link: https://cdn.aigroup.com.au/Submissions/Technology/AiGroup_submission_Digital_Platforms_Inquiry.pdf.
[2] Commonwealth Attorney-General, *Review of the Privacy Act 1988*, Link: https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988.
[3] 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.
[4] 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.

- Home Affairs's consultation on its draft *Critical Technology Supply Chain Principles* – a range of matters including principles that may be applicable to these reforms.[5]

- 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.[6]

- Treasury's consultation on its *Inquiry into Future Directions for the Consumer Data Right* – we raised several interrelated issues including on privacy, data protection and cyber security.[7]

- Treasury's consultation on *Improving the Effectiveness of the Consumer Product Safety System* – critical infrastructure and assets may also fall under the scope of Treasury's consultation if it leads to consumer safety issues.[8]

- PJCIS and INSLM reviews relating to the TOLA Act – there are concerns about the potential negative impact of this Act on cyber security and privacy of products and services.[9] We have recently made a supplementary submission supporting the INSLM's recommendations.[10]

- 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.[11]

- 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.[12]

- The Ambassador for Cyber Affairs and Critical Technology within DFAT has been consulting on *Australia's International Cyber and Critical Technology Engagement Strategy*, which will potentially be relevant to these reforms.[13]

---

[5] Ai Group submission to Home Affairs (November 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Home_Affairs_Critical_Technology_Supply_Chain_Principles_Discussion_Paper_12Nov.pdf.

[6] Ai Group submission to Treasury (September 2020), Link: https://cdn.aigroup.com.au/Submissions/Trade_and_Export/Submission_FATA_reforms_September_2020.pdf.

[7] Ai Group submission to Treasury (June 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Treasury_CDR_Inquiry_5Jun_2020.pdf.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

- 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*, and its recently commenced consultation on an *AI Action Plan*.[15]

Recommendation: Coordination be undertaken by Home Affairs and other relevant Government Departments to enable for proper consultation for both this consultation and others underway.

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, *Australia's AI Action Plan*, Link: https://www.industry.gov.au/news/australias-ai-action-plan-have-your-say.