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 February 2021

Senator James Paterson, Chair
Parliamentary Joint Committee on Intelligence and Security
Email: pjcis@aph.gov.au

Dear Senator Paterson

REVIEW OF THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review into the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Bill).

1. Consultation process

We note that the PJCIS's review of the Bill follows the consultation by the Department of Home Affairs (Home Affairs) on its Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Exposure Draft Bill), under 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 the PJCIS's review of the Bill.

In our previous submission to Home Affairs (towards the end of November last year), we strongly recommended that the PJCIS and Independent National Security Legislation Monitor (INSLM) be included as part of the review of the Bill should the Exposure Draft Bill reach the stage for Parliamentary consideration. However, we suggested that moving the Bill to Parliamentary stage would be premature for various reasons outlined in our submission.

Given the deadline for submissions to Home Affairs on the Exposure Draft Bill (27 November 2020) and the date that the Bill was introduced into Parliament (10 December 2020), we are not confident that our concerns have been properly taken into consideration in such a short period of time.

While we appreciated the opportunity to comment on the previous Exposure Draft Bill, we noted that this was the first real opportunity to comment on the detail of a technically complex and detailed piece of proposed legislation. Upon reviewing the documents associated with that Exposure Draft Bill, we considered that these raised more questions for industry. We therefore expect similar issues will arise with the latest iteration of the Bill.

As a result, we strongly considered that additional time was needed for deeper consultation on the Exposure Draft Bill, consideration of legitimate comments arising from that 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 the Exposure Draft Bill was also 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 by the PJCIS for this latest review, the PJCIS is also currently reviewing the

TSSR. It is therefore important that relevant matters arising from the TSSR review, other reforms and initiatives, and existing arrangements are appropriately considered.

Generally, 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 with Home Affairs.

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 Home Affairs, PJCIS and other relevant government departments and agencies on these reforms.

In the meantime, we would like to reiterate in this submission our preliminary views raised at the Exposure Draft Bill stage, which we consider to be relevant for the PJCIS's review of the Bill in light of the short timeframe between the Exposure Draft Bill and Bill stages.[1] We also elaborate further with additional comments since our previous submission in November last year.[2] As further consultation is undertaken, there may be other matters raised.

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

2. Regulatory Impact Statement (RIS)

As stated in the previous Draft Explanatory Document, the Explanatory Memorandum indicates that a qualitative RIS has been undertaken on the potential costs and benefits of the proposed reforms. It also proposes that a more accurate RIS with quantitative cost-benefit assessment with respect to the Positive Security Obligation component will be undertaken when sector-specific rules are being developed. We understand from the previous Draft Explanatory Document that this will not occur until after the legislation is passed.

With respect to the Enhanced Cyber Security Obligations, the previous Draft Explanatory Document indicated that a quantitative cost-benefit assessment will be provided upon commencement of the legislation with respect to these Obligations, expansion of the critical infrastructure assets register, and mandatory cyber incident reporting. This inferred 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.

We note that the Explanatory Memorandum now includes some form of cost-benefit assessment with respect to Enhanced Cyber Security Obligations. However, we do not consider that stakeholders have been given sufficient time to scrutinise the assessment including estimated costs, assumptions made and extent of individual consultation. It can be inferred that the costs are realistically unknown according to the following statement in the Explanatory Memorandum: "The regulatory costs of imposing Enhanced Cyber Security Obligations would vary widely depending on the scope of the obligations and the individual circumstances of the entity subject to the obligations. The obligations will only be enlivened on request." The Explanatory Memorandum also makes a similar statement with respect to costs associated with Government Assistance measures.

Where proposed legislation establishes a broad framework for future regulation, we appreciate that 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) that it wishes to take to enable these to be assessed alongside the enabling legislation.

---

[1] With respect to the PJCIS's statutory review of the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act), we do not provide specific comments in this submission. However, we consider that the concurrent reviews of the existing Act and proposed Bill are closely interrelated, and therefore amendments arising from the Bill are likely to be relevant to this statutory review of the Act.

[2] A copy of Ai Group's submissions to Home Affairs on the PCISNS reforms can be found here: https://cdn.aigroup.com.au/Submissions/Technology/Home_Affairs_Critical_Infrastructure_Security_Reforms_Exposure_Draft_Bill_Nov2020.pdf; and https://cdn.aigroup.com.au/Submissions/Technology/Dept_Home_Affairs_Critical_Infrastructure_Security_Reforms_Sept2020.pdf.

Further, we are extremely uncomfortable with proposed reforms that have not been subject to a proper cost-benefit assessment and adequate time for relevant industry scrutiny, 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 and consultation. 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.[3]

- 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 (e.g. details in sector specific rules that are currently unknown) 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 Bill

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

[3] For example, an energy industry member suggested in one of our previous submissions that existing regulators in the energy sector have not been favourable to increasing spending in cyber security, including the latest Australian Energy Regulator (AER) regulatory determinations for electricity distribution network businesses. It is unclear if this will change as a result of these critical infrastructure security reforms. However, it is clear that the current frameworks for assessing the costs and funding for cyber security for regulated entities in the energy sector is not aligned with increased cyber security capability. This will need to change if these reforms are to succeed.

However, we still consider that further clarification is still required with respect to the Bill. Previously highlighted areas of uncertainty that still require further clarification include the nature of the reforms, scope, definitions, measures and cost-benefit impact. We elaborate further with examples below.

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

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

3.1 Scope of sectors and critical assets

The Bill attempts to provide some clarity on sectors and assets that are subject to the proposed requirements. However, more improvement can be made to clarify these definitions.

For instance, 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 Bill, including 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.

In the case of "data storage or processing", this definition is still vague as many businesses may have data storage or processing, as part of their business models. As an example, we discuss later in this submission about problems for these types of companies with respect to Positive Security Obligations (PSO).

Another example is the food and groceries sector. A member in that sector provided the following comments:

> *It would be useful for the Bill to identify the relevant food and groceries by reference to what is "critical". One way to do this would be to define food as "critical food items (including fresh and long-life products), pet food, non-alcoholic drinks, cleaning products, toiletries and pharmaceuticals". This approach would also have the benefit of drawing on an established framework, understood by market participants.*
>
> *An unduly broad approach to defining "food" (i.e. by reference to anything for human consumption) puts in question the ability of supermarkets and wholesalers to achieve the Bill's objective. Supermarkets and wholesalers need to have sufficient flexibility to respond to significant incidents. This includes refocusing arrangements to maximise supply of those specific food and grocery items identified as critical to the well-being of Australians.*
>
> *Our concern is that there are some products in our supply chain which are just not critical but without limiting the scope and being clear, we could end up having to risk mitigate for all items in the food and grocery sector.*

The member also suggests an opportunity to clarify the relationship between the concept of "network" and "critical assets" in terms of "critical food and grocery asset" through an amendment to section 12K of the Bill:

> *We understand that the intention is to capture those assets which are, in the responsible entity's opinion, critical to the network that enables the supply of food and groceries to end-customers, including transport and distribution facilities.*
>
> *It may be appropriate to consider the following amendments to clarify this intention:*
>
> - *Amend section 12K(1) to read "An asset is a critical food and grocery asset if it is critical to a network that:..". This will make it clear that an asset is a component of the food or grocery distribution or supply network, rather than the network itself.*

- *Change the three references to "network" in section 12K(2) to "part of" a network i.e. section 12K(2)(a) would read "a part of a network is used...".*

- *Amend section 12K(2)(b) to read "that part of the network is operated under a contract on behalf of an entity referred to in paragraph (1)(b);". This will clarify that the sub-section is also intended to apply in those circumstances where only a part of the network is operated under a contract.*

3.2 Scope of entity responsibility

Risk management obligations have been proposed as part of the PSO in the Bill (we discuss broader issues with the PSO later in this submission). Setting aside these overall concerns with the PSO for the moment, this section discusses the scope of entity responsibility and uses risk management obligations as an example if these were to be introduced through the Bill.

Should such obligations be defined in the Bill, there needs to be proper consideration on the extent of entity responsibility based on what is within the entity's 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. In this regard, we suggest that the responsible entity would likely be best placed to understand and define what is critical in this context. We discuss these issues further below.

3.2.1 Materiality threshold for risk impact

We understand that the intention of Part 2A of the Bill on critical infrastructure risk management programs is to ensure that responsible entities focus their attention on managing the risks associated with significant disruption to critical assets. For example, this could mean taking steps to prevent a serious disruption to supply or distribution. That is, a real risk (probability) of a significant event occurring (hazard) that has a material consequence.

The Bill refers to "material risks" of "any hazard" occurring, which could have a "relevant impact" (cf Part 30AA of the Bill). In turn, a relevant impact is defined in section 8G of the Bill to refer to "any impact … on availability", "any impact ... on reliability" etc.

It is important to include a materiality qualifier about the hazard and relevant impact (the consequence), not just the risk (the probability). Examples of how this could be addressed may entail:

- Inserting the word "material" before "impact" in paragraphs (1)(a)-(d), (2)(a)-(d) and (3)(a)-(d) of section 8G of the Bill e.g. "the material impact (whether direct or indirect) of the hazard on the availability of the asset".

- Amending section 30AA of the Bill to read:

  …
  The purpose of a critical infrastructure risk management program is to do the following for each of those assets:

  *(a) identify each **material** hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;*

  (b) so far as it is reasonably possible to do so—minimise or eliminate any material risk of such a hazard occurring;

  (c) mitigate the relevant impact of such a hazard on the asset.
  …

- Including sector-specific guidance for materiality in the rules.

A related point is the obligation to notify of "cyber security incidents" under section 30BC of the Bill. We suggest this obligation be clarified to ensure it only applies to cyber security incidents that introduce a risk of a material impact.

In each case, we note that what is "material" for a given sector could be defined in the rules (rather than the legislation). However, it would be more preferable if this is defined in legislation rather than rules or regulations to provide more certainty.

3.2.2 Defining critical supply chain

Among other things, there is a need for further clarity on definitions or guidance relating to the "supply chain". Transparency and certainty would be enhanced if the scope of this definition was better defined in the legislation. This is important to properly understand and identify risk management obligations.

An option is to make it clear under Part 2A of the Bill that risk management obligations for targeted entities are limited to critical goods or services that are within their immediate control. For example, the risk management obligations for the targeted entity:

- commence from the point that critical goods or services are supplied into the entity's network and under its immediate control; and

- do not include activities beyond the entity's immediate control – using the food and grocery sector as an example, this could mean food production, manufacturing or packaging or the acquisition of food and groceries from third parties.

We consider the above approach warrants further consideration as an option and consultation with relevant stakeholder feedback for their respective sectors.

4. Positive Security Obligations (PSO)

4.1 Support for the intent

We welcome the Government's acknowledgement in the Explanatory Memorandum 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 these 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;

- mandatory reporting of 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 has been 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 this work to develop further detail and the scope 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 Explanatory Memorandum, 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".

In implementing a non-regulatory approach, we recommend consideration be given to referencing appropriate standards, which would provide Government and private sector confidence in the PSO. This can enable maturity modelling that reflects the level of security maturity required to effectively manage risk, and self-regulation through assurance against such standards 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 Explanatory Memorandum suggests that this "will support the development of an aggregated threat picture to inform both proactive and reactive cyber response options – from providing immediate assistance 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.

This is further complicated by the requirement for the entity to provide sufficient information on a regular basis to sustain an all-hazards risk management system. Such a risk management requirement will likely require businesses to have significant resources, with a greater burden placed on smaller businesses. To address this, an option for further consideration should be given to enhanced threat and hazard assessments by the Government; this could help to create a timely and comprehensive assessment of the threat and hazard environment, and determine specific consequences if the threat is realised.

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 cyber risk management program, or advise the entity of its security risk considerations having regard to its ownership and operational information?

Further, to adequately assess risk in an all-hazards approach, all relevant agencies should be involved including: ASD, ASIO and AFP for security related threats; and other Government agencies such as Emergency Management Australia, Geoscience Australia and Bureau of Meteorology for other types of threats.

Recommendations:

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

- **A mutual obligation be created for other relevant agencies including ASIO and AFP to assist the entity if the entity is obligated to maintain a risk management system for PSO controls, cybersecurity and resilience, or when there is 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 Explanatory Memorandum states that the definition of such incidents is not defined as their significance may vary between assets. This would be left to the judgement of the entity with sector specific guidance to be developed between the Department and industry. 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)

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

On the one hand, the Explanatory Memorandum 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 Explanatory Memorandum 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 Explanatory Memorandum appears to deem that

the existing Defence security mechanisms under the DISP are appropriate insofar as it relates to the PSO, it is not clear whether this extends to the application of the ECSO and Government Assistance measures for the defence sector. The previous Draft Explanatory Document had explicitly stated that the ECSO (if any critical defence assets are designated as systems of national significance) and Government Assistance measures would still apply for the defence sector but this appears to now be omitted from the Explanatory Memorandum. At the time, it was not altogether clear why the ECSO and Government Assistance measures were required for the defence industry, given Home Affairs's acceptance of the DISP. With this no longer explicitly mentioned in the Explanatory Memorandum, it is unclear whether these proposed obligations still apply to the defence sector.

The ECSO also includes an obligation where the Home Affairs Secretary may require an entity to provide it with access to 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 Explanatory Memorandum 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 to assist in protecting our critical infrastructure. We appreciate the hypothetical scenarios provided in the Explanatory Memorandum to help in clarifying by way of examples of when, where and how Government could undertake Government Assistance.

However, there are still 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 Explanatory Memorandum 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 Explanatory Memorandum 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 responding to a cyber security incident, the Explanatory Memorandum notes that "Due to rapid technological change, it is not possible to foresee all possible ways that a system may be compromised or exploited, or the actions that would be required to respond to the incident. In particular, the methods of compromise and the required responses will change over time alongside technology. Therefore, a non-prescriptive approach has been taken in relation to defining what a response to a cyber security incident would involve. Further, it is important to recognise that a response will be proportionate to the nature of the incident and the system that will, is being, or has been, impact, as well as impacted by the capabilities of

the entity responsible for protecting the system." However, this creates uncertainty for a direction that should be triggered in very limited circumstances (i.e. emergency) and therefore not be broadly interpreted.

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

- The lack of accountability 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. This infers that Government recognises that risk of errors could arise and therefore 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 stakeholders, potentially suffering consequences such as increased cost of capital as shareholders perceive such risk, increased insurance costs, or relocation of investment overseas. This will need to be included as part of any cost-benefit assessment (as noted above). Further, we propose that the PJCIS should recommend that the Government be required to reimburse affected private entities for damages caused in the process of executing a Government directive where the Government takes emergency action on an entity's network.

- For smaller entities in particular sectors that may be subject to these Government Assistance measures, we suggest consideration should be given as to the proportionality of executing these measures and a potentially greater regulatory burden and cost that this would be placed on such entities; for example, whether the powers should be limited to a certain class of entity.

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 in the Bill, 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 Bill proposes to exempt ministerial authorisations and administrative decisions made under these powers from being subject to judicial review. Some reasons provided in the Explanatory Memorandum for seeking exemption from judicial review are that "This is reflective of the emergency nature of these powers, national security information that will used to satisfy the various decision makers, and their connection with the protection of Australia's national security, defence, economy and social stability."

Instead, the Explanatory Memorandum suggests that there are certain safeguards and limitations that would be included in the Bill to ensure that any Commonwealth decisions made through Government Assistance measures are appropriate.

While we understand this rationale, we do not consider that the Government offers a satisfactory level of assurance to industry. There should be further consideration of other options for providing adequate independent oversight while also addressing the Government's needs. For example, similar considerations were given during the TOLA Act Review by the INSLM in consultation with a wide range of stakeholders. We endorsed 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 PCISNS 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 Bill's 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 the 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. 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.

For example, the Explanatory Memorandum 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, Parliament has recently passed through changes to the *Foreign Acquisitions and Takeovers Act 1975* (Cth) (FATA) that would subject any business responsible for, or with a significant stake in, critical infrastructure covered by the SOCI Act to substantial new obligations and powers under the FATA. Thus decisions about the scope of the SOCI Act will have larger implications that need to be fully considered in a regulatory impact analysis.[4]

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

- ACCC *Digital Platforms Inquiry* – Government's response to this Inquiry includes policy reforms in the area of privacy and data regulation.[5] Following this Inquiry, the Attorney General's Department has now commenced its *Review of the Privacy Act*. [6]

- Department of Infrastructure, Transport, Regional Development and Communications consultation on a new *Online Safety Act* – online safety proposals in this consultation may be relevant to these reforms.[7]

- Home Affairs *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.[8]

[4] Ai Group submission to Treasury (September 2020), Link: https://cdn.aigroup.com.au/Submissions/Trade_and_Export/Submission_FATA_reforms_September_2020.pdf.
[5] Ai Group submission to Treasury (September 2019), Link: https://cdn.aigroup.com.au/Submissions/Technology/AiGroup_submission_Digital_Platforms_Inquiry.pdf.
[6] Ai Group submission to Attorney-General's Department (November 2020), Link: https://cdn.aigroup.com.au/Submissions/General/2020/Privacy_Act_Review_November_2020.pdf.
[7] Ai Group submission to Department of Infrastructure, Transport, Regional Development and Communications (February 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/New_Online_Safety_Act_Proposals_21Feb_2020.pdf.
[8] 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 consultation on its draft *Critical Technology Supply Chain Principles* – a range of matters including principles that may be applicable to these reforms.[9]

- Treasury 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.[10]

- Treasury 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.[11]

- 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.[12] We made a supplementary submission supporting the INSLM's recommendations.[13]

- PJCIS review into the effectiveness of the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* – we consider this review interrelated with the TOLA Act review.[14]

- 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.[15]

- Ambassador for Cyber Affairs and Critical Technology within the Department of Foreign Affairs and Trade has been consulting on *Australia's International Cyber and Critical Technology Engagement Strategy*, which will potentially be relevant to these reforms.[16]

- Australian Human Rights Commission (AHRC) consultation into *Human Rights and Technology* – as the title suggests, the AHRC have been exploring the impact of emerging technologies on human rights.[17]

- Department of Industry, Science, Energy and Resources AI initiatives such as the *AI Ethics Framework*, and its recently commenced consultation on an *AI Action Plan*.[18]

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

---

[9] 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.
[10] Ai Group submission to Treasury (June 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Treasury_CDR_Inquiry_5Jun_2020.pdf.
[11] Treasury, *Improving the Effectiveness of the Consumer Product Safety System*, Link: https://consult.treasury.gov.au/market-and-competition-policy-division-internal/main-consultation.
[12] Joint submission to PJCIS (Submission No. 23, July 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions; Joint submission to the INSLM (Submission No. 15, September 2019), Link: https://www.inslm.gov.au/submissions/tola; Ai Group submission to the INSLM (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.
[13] 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.
[14] 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.
[15] Ai Group submission to Standing Committee on Communications and the Arts (Submission No. 356, November 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Communications/5G/Submissions.
[16] Department of Foreign Affairs and Trade, *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] Ai Group submission to AHRC (March 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/AHRC_Human_Rights_and_Technology_Discussion_Paper_26Mar_2020.pdf.
[18] Ai Group submission to Department of Industry, Science, Energy and Resources (December 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/DISER_AI_Action_Plan_Dec2020.pdf.

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, [redacted],
[redacted]

Yours sincerely,

[redacted]

Louise McGrath
Head of Industry Development and Policy