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

25 February 2022

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 PROTECTION) BILL 2022 (CTH)

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on its review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (Cth) (SLACIP Bill).

Ai Group's 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.

Overall, Ai Group is supportive of the intent behind the Bill. However, as previously raised in submissions related to the package of critical infrastructure security reforms over the last several years, we consider there are several outstanding matters that need to be addressed in the latest Bill. This was most recently raised in our submission to the Department of Home Affairs (Home Affairs) on its consultation on the SLACIP Bill Exposure Draft, which closed on 1 February 2022.

For the purposes of the PJCIS's review, we are responding to the PJCIS's principle-based questions and have included a reproduced copy of our submission to Home Affairs in Appendix A.

We would also welcome our continued inclusion in further consultations and the opportunity to work closely with relevant members covering a wide range of sectors that may be captured by these reforms, Home Affairs, PJCIS and other relevant government departments, agencies and authorities.

1. **PJCIS Question:** ***Did you provide feedback on the exposure draft and do you feel like consultation was inclusive and wide-ranging?***

Generally, we have welcomed the consultative approach that Home Affairs undertook in holding virtual town halls, industry specific workshops and roundtables as part of the reform process. We encourage that this level of stakeholder engagement continues with Home Affairs. However, we consider that the limited timeframe scheduled for consultation (especially concurrent consultations) and development of the SLACIP Bill leaves room for improvement. The timing of this particular consultation has also been especially difficult during the Christmas-New Year break, as well as coinciding with the Omicron outbreak, that would have likely impacted on stakeholder engagement.

We therefore strongly consider that additional time and consultation stages are needed for deeper consultation on the SLACIP Bill, including with any associated clarifying rules. This will enable proper consideration of legitimate comments arising from such consultation, and responsive amendments to, and sufficient scrutiny of, the Bill. We discuss in further detail about this issue in our submission to Home Affairs (see pages 2-4 in Appendix A).

In addition, we note that the Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022 (Cth) has recently been introduced into Parliament on 17 February 2022,[1] following the Government's

[1] See: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6855.

Ransomware Action Plan announcement in October 2021.[2] Treasury is also concurrently consulting on a Discussion Paper and Exposure Draft Regulations as part of its 2022 Foreign Investment Reforms, with consultations commencing on 14 February 2022.[3] This reinforces our recommendation that interrelated and concurrent reforms need to be properly coordinated and consulted with relevant stakeholders.

2. PJCIS Question: ***Has your feedback been incorporated in the Bill or addressed in explanatory material?***

Our feedback regarding outstanding matters in the SLACIP Bill is summarised in our submission to Home Affairs (pages 1-2 of Appendix A), with more specific detail in the remainder of that submission.

Given the tight timeframe between submissions to Home Affairs' SLACIP Bill consultation (closed 1 February 2022) and the PJCIS's review (commenced 11 February 2022), we are uncertain whether Home Affairs has had sufficient time to address our issues and recommendations (amongst other submissions). We would welcome clarification from the Government on how it considers these have been addressed.

In addition, there are issues and recommendations that we previously raised in our February 2021 submission to the PJCIS with the objective of providing better clarity and safeguards that may warrant further review. For instance, we offered examples of how materiality for risk management obligations and notifying of cyber incidents could be assessed and clarified in legislation and rules.[4] There should also be appreciation that the nature of material risk can vary depending on a range of factors including the sector, asset, supply chain and entity. Furthermore, if Government were to be given the power to intervene and deem particular risks as material and place mandatory obligations on entities through their Risk Management Programs,[5] there should be appropriate safeguards in place e.g. transparency in Government decision-making through objective criteria.

3. PJCIS Question: ***What are your five key themes of feedback on the Bill?***

Our issues and recommendations regarding the SLACIP Bill (as raised in our submission to Home Affairs) can be grouped into the following themes:

i. **Process:** Need for proper consultation on critical infrastructure reforms and coordination between interrelated reforms;

ii. **Scope and impact:** Need for clarification on scope of businesses covered and their obligations (and how they are assessed and determined), and proper regulatory impact assessment;

iii. **Regulatory responsibilities and oversight:** Need for clarification on regulators' mutual obligations, and implementation of proper regulatory safeguards and oversight; and

iv. **Remedies:** Need for proper understanding of existing legislative/regulatory requirements or obligations to avoid duplication, consideration of non-regulatory options and understanding the objective of civil penalties.

4. PJCIS Question: ***Do you think the potential regulatory impact has been captured accurately?***

As previously stated, the challenge with these reforms is providing meaningful comments on the impact (including regulatory costs) on a Bill that requires further detail (e.g. via clarifying rules). As one member previously commented, it is impossible to estimate costs of such measures without the detail.

[2] Minister for Home Affairs, "New plan to protect Australians against ransomware" (13 October 2021, Media Release), https://minister.homeaffairs.gov.au/KarenAndrews/Pages/new-plan-to-protect-australians-against-ransomware.aspx.
[3] See: https://treasury.gov.au/consultation/c2022-244363; and https://treasury.gov.au/consultation/c2022-244363-edr.
[4] Ai Group submission to PJCIS (No 41, February 2021), pp. 5-6, Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/SOCI/Submissions.
[5] Explanatory Memorandum to the SLACIP Bill, p. 46, para 223.

In our submission to Home Affairs, we suggest various factors that should be taken into consideration in a regulatory impact assessment. Please refer to pages 9-10 of Appendix A for further detail.

5. PJCIS Question: *On balance, do you support the Bill in its presented form, recognising the risks facing critical infrastructure assets in Australia?*

In principle, we support the intention behind the SLACIP Bill (as well as *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth) (SLACI Act)). However, as raised in our submission to Home Affairs, there are a range of areas regarding the Bill that need to be worked through between Government and relevant stakeholders to provide better clarity and address other outstanding matters.

If you would like clarification about this submission, please do not hesitate to contact me or Charles Hoang (Lead Adviser – Industry Development and Defence Industry Policy, [redacted].

Yours sincerely,

[redacted]

Louise McGrath
Head of Industry Development and Policy

Appendix A: Ai Group submission to Home Affairs on Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (Cth), 1 February 2022 [REPRODUCED COPY]

1 February 2022

Cyber and Infrastructure Security Centre
Department of Home Affairs
Email: CI.Reforms@homeaffairs.gov.au

Dear Sir/Madam

EXPOSURE DRAFT SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE PROTECTION) BILL 2022 (CTH)

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission to the consultation on the Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (Cth) (SLACIP Bill) by the Department of Home Affairs (Home Affairs).

Overall, Ai Group is supportive of the intent behind the Bill. However, as previously raised in submissions related to the critical infrastructure security package of reforms over the last several years, we consider there are several outstanding matters that need to be addressed in the latest Bill.

Below is a summary of our issues and recommendations.

Issues	Recommendations
1. Concurrent consultations	• The SLACIP Bill should include draft clarifying rules as part of this consultation to enable proper assessment of the details associated with the Bill. • Sufficient time and consultation stages need to be allocated for providing proper stakeholder consultation on the concurrent package of critical infrastructure security reform consultations currently underway, including the SLACIP Bill and associated rules.
2. Interrelated reforms	• Government should give proper consideration to the interrelated reforms, legislations and regulations relevant to this consultation, and their impact on businesses including uncertainties that may be introduced, chilling investment and innovation. • Government should improve coordination between government departments, agencies and authorities with respect to this consultation and other interrelated reforms, legislations and regulations. For example, consider establishing a central regulatory body (such as under the PM&C) for coordinating between the various regulators with respect to these types of interrelated reforms.
3. Potential breadth of entities covered	• Further clarity be provided on the entities covered and not covered in these reforms.
4. Potential duplication of existing requirements	• A thorough gap analysis and assessment be undertaken on the proposed obligations in the SLACIP Bill against existing obligations across the various sectors.
5. Non-regulatory options	• Non-regulatory options be considered as alternatives to the proposed obligations under the SLACIP Bill.
6. Mutual obligations	• 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.
7. Civil penalties	• The purpose behind the proposed new legislative provisions including civil penalty provisions be reviewed, and other options be considered.

Issues	Recommendations
8. Safeguards and oversight	• 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. • Clarity be provided about the impact on liability and insurance as a consequence of following Government directions.
9. Regulatory impact assessment	• Government undertakes a proper quantitative cost-benefit assessment for the proposed reforms prior to making legislation.

1. Consultation process

1.1 Concurrent consultations

We note that this consultation follows the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth) (SLACI Act) that the Government states was built on existing requirements under the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act), and was passed through Australian Parliament in November 2021 and commenced operation in December 2021.

Concurrent to this, we note that the Government is separately consulting on its Transport Security Amendment (Critical Infrastructure) Bill 2021 (Cth) (TSACI Bill), with an exposure draft of the Bill also released for public consultation and due on the same day (1 February 2022). We understand that the TSACI Bill progresses reforms to Australia's critical infrastructure security framework by amending the *Aviation Transport Security Act 2004* (Cth) and *Maritime Transport and Offshore Facilities Security Act 2003* (Cth).

Finally, Home Affairs is also concurrently consulting on two draft rules for two new Positive Security Obligations (PSOs) i.e. the register of critical infrastructure assets and mandatory cyber security incident reporting, also due on 1 February 2022.

Prior to the SLACI Act, we expressed concerns during the consultation process that the Bill did not address various areas of uncertainty and it was premature to have the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (SLACI Bill 2020) tabled into Parliament in December 2020.

We acknowledge that Home Affairs consulted through workshops concurrently to the SLACI Bill 2020 on sector specific rules with the electricity and gas sectors being the first sectors, followed by the data storage and processing, and water sectors. However, other identified sectors in the Bill were yet to be considered. As part of these reforms, Home Affairs also consulted last year on generic governance rules, and critical asset definitions and rules. These concurrent consultations were undertaken in anticipation of the legislation being passed through Australian Parliament.

Our preference would have been for these consultations, especially on sector specific requirements, to have occurred prior to the SLACI Bill 2020 being tabled into Parliament. This may have assisted stakeholders to gain a better understanding of the specific requirements that may or may not apply to their specific sectors and businesses.

Understandably, there were many relevant and important questions and ideas about the SLACI Bill 2020 raised by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and stakeholders during its public hearing in July 2021. This may have been due to issues and options not having been properly worked through before it was originally tabled into Parliament.

Despite these concerns, the Government decided to split the SLACI Bill 2020 into two, following recommendations made by the PJCIS, with "the 'urgent elements of the reforms' [to] be 'legislated in the shortest possible time'".[6]

Given these parallel reforms, there will also likely be confusion and complexity for all parties (including policy makers, authorities and stakeholders) regarding the implementation of these reforms. Now with

[6] Explanatory Document to SLACIP Bill, p. 5.

the SLACI Act in operation, the current amended version of the SOCI Act must be complied with as a result; at the same time, this same piece of legislation could be subject to change again, depending on the outcomes of the SLACIP Bill.

While the SLACI Act is in operation, we consider that further clarification is still required and therefore associated clarifying rules need to be included as part of the SLACIP Bill consultation process. Supporting this, we note that the PJCIS recommended in its Advisory Report to its review of the SLACI Bill 2020 that: "any rules to be designed under Bill Two be co-designed, agreed and finalised to the extent possible before the introduction of that Bill and made available as part of the explanatory material for the Bill".[7] Instead, fundamental issues remain outstanding. For example, it is not clear what decision-making criteria would be applied in declaring a "System of National Significance" and so it is unclear to what extent the Enhanced Cyber Security Obligations (ECSO) would apply to entities.

We therefore strongly consider that additional time and consultation stages are needed for deeper consultation on the SLACIP Bill, including with any associated clarifying rules. This will enable proper consideration of legitimate comments arising from such consultation, and responsive amendments to, and sufficient scrutiny of, the Bill.

Generally, we have welcomed the consultative approach that Home Affairs has undertaken in holding virtual town halls, industry specific workshops and roundtables as part of the reform process. We encourage that this level of stakeholder engagement continues with Home Affairs. However, we consider that the limited timeframe scheduled for consultation (especially concurrent consultations) and development of the SLACIP Bill leaves room for improvement.

We also welcome our ongoing inclusion in further consultations, along with relevant members covering a wide range of sectors that may be captured by these reforms, and continuing to work closely with Home Affairs, PJCIS and other relevant government departments, agencies and authorities on these reforms.

Ai Group recommendations:

- ***The SLACIP Bill should include draft clarifying rules as part of this consultation to enable proper assessment of the details associated with the Bill.***
- ***Sufficient time and consultation stages need to be allocated for providing proper stakeholder consultation on the concurrent package of critical infrastructure security reform consultations currently underway, including the SLACIP Bill and associated rules.***

1.2 Interrelated reforms

In addition to the SLACI Act and other concurrent critical infrastructure security reform consultations, there are also other interrelated reform activities that need to be accounted for; some of which we have previously raised.[8] We consider these still pertinent to these latest reforms.

For example, the Australian Parliament passed through changes to the *Foreign Acquisitions and Takeovers Act 1975* (Cth) (FATA) in December 2020 that subjects 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 reforms. With the changes made from the SLACI Act, expanding the coverage of the framework from four sectors (water, electricity, gas and ports) to 11 sectors and 22 asset classes, the scope of the FATA reforms has also been automatically expanded as a consequence. As previously raised during this consultation, decisions about the scope of the SOCI Act has larger implications that need to be fully considered in a regulatory impact analysis.[9]

[7] PJCIS Advisory Report to the SLACI Bill 2020, p. xix.
[8] Ai Group submission to PJCIS (No. 41, February 2021), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/SOCI/Submissions.
[9] Ai Group submission to Treasury (September 2020), Link: https://cdn.aigroup.com.au/Submissions/Trade_and_Export/Submission_FATA_reforms_September_2020.pdf.

We also note that the Attorney-General's Department is currently undertaking a review of the *Privacy Act 1998* (Cth), which may impact how entities comply with the SLACI Act and SLACIP Bill.[10] An outcome of the review may result in the expansion of the definition of "personal information" to include technical information in the Privacy Act. Therefore, if such changes were to arise from the privacy reforms, the critical infrastructure security reforms will need to properly take these privacy changes into account e.g. how the proposed step-in rights would impact on privacy when managing an incident.

We therefore continue to recommend coordination be undertaken by Home Affairs (including Cyber and Infrastructure Security Centre) and other relevant government departments, agencies and authorities to enable for proper consultation for both this consultation and others underway.

Proper stakeholder consultation on these interrelated reforms could include assessing the merits of establishing a central regulatory body (under a central government department such as the Department of the Prime Minister and Cabinet (PM&C)) that can properly coordinate between the various regulators responsible for developing codes and regulations. This could enable a more holistic consideration including understanding the cumulative regulatory impacts and costs on affected stakeholders who may be subject to multiple regulations related to online activities. The PM&C also plays an important role, providing oversight of the Digital Economy Strategy, Australian Data Strategy and most recent Critical Technologies Blueprint and Action Plan, so this coordinating approach could be another advantage.

Ai Group recommendations:

- ***Government should give proper consideration to the interrelated reforms, legislations and regulations relevant to this consultation, and their impact on businesses including uncertainties that may be introduced, chilling investment and innovation.***
- ***Government should improve coordination between government departments, agencies and authorities with respect to this consultation and other interrelated reforms, legislations and regulations. For example, consider establishing a central regulatory body (such as under the PM&C) for coordinating between the various regulators with respect to these types of interrelated reforms.***

2. Outstanding matters

According to the Explanatory Document to the SLACIP Bill, the SLACI Act amended the SOCI Act to "incorporate 'government assistance measures' that provide a legislated response to a significant cyber incident, cyber incident reporting obligations, expanding the definition of critical infrastructure to include 11 sectors, and associated definitions and powers".[11]

The SLACIP Bill seeks to amend the SOCI Act "to capture the remaining elements from the SLACI Bill 2020 together with amendments suggested by stakeholders and throughout the Parliamentary Joint Committee on Intelligence and Security review process, including: the Risk Management Program under proposed Part 2A; enhanced cyber security obligations under proposed Part 2C; Systems of National Significance under proposed Part 6A; and information sharing provisions for regulated entities".[12]

Noting that the SLACI Act has commenced operation, we will aim to focus on elements of the SLACIP Bill. However, there are outstanding matters that apply to both the SLACI Act and SLACIP Bill, which we consider should be reviewed as a matter of good regulatory and policy practice to ensure consistency in approach.

[10] See: https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/.
[11] Explanatory Document to SLACIP Bill, p. 5.
[12] Explanatory Document to SLACIP Bill, p. 5.

In addition to the consultation process matters discussed above, the following is a list of key areas that Ai Group previously raised in our submissions regarding the SLACI Bill 2020, which we continue to stand by, including with respect to:[13]

- Potential breadth of entities covered;
- Potential duplication of existing requirements;
- ECSO, including non-regulatory options, mutual obligations and civil penalties;
- Safeguards and oversight; and
- Regulatory impact assessment.

Given the relevance of these issues to the latest Bill, we reiterate these issues below.

2.1 Potential breadth of entities covered

Several proposal obligations under the legislation and rules, particularly ECSO, will depend on whether or not an entity is defined as a "System of National Significance". It is critical that more certainty is provided, including the criteria that must be assessed for determining whether to declare a "System of National Significance".

In this regard, the challenge with these reforms is providing meaningful comments on the impact (including regulatory costs) on a Bill that requires further detail. As one member previously commented, it is impossible to estimate costs of such measures without the detail.

We are concerned 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 (but not limited to) suppliers, manufacturers and the "data storage or processing" sector. There is also a potentially higher regulatory burden created for small and medium enterprises and those not currently subject to critical infrastructure security legislation. And there is also a need to understand the extent of entity responsibility based on what is within the entity's control (including scope of critical assets and supply chains), as well as related matters such as the scope of responsibility of an entity that may flow down the supply chain.[14]

Ultimately, the scope and impact of the Bill will largely be contingent on clarifying its various aspects that may include (but not limited to) properly defining targeted entities and sectors, sector specific requirements, entity responsibilities and obligations, critical supply chains, critical assets, and a range of other matters that have been previously raised by stakeholders. Clarifying these matters should assist in providing more regulatory certainty for stakeholders that may be affected, and in better understanding the regulatory impact of the Bill such as potential costs. It should also help to minimise the risk of duplicating existing requirements and assist relevant government departments, agencies and authorities (including regulatory bodies) in understanding their roles should such a Bill be implemented.

For example, regarding the proposed changes to the definition of "data storage or processing service" and "data storage and processing asset", these should be clarified further to assist in better identifying

[13] See our previous submissions on the SLACI Bill 2020 for further information: Submissions to PJCIS (No 41 and 41.1, February and July 2021, respectively), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/SOCI/Submissions; Submission to Home Affairs (May 2021), Link: https://www.aigroup.com.au/globalassets/news/submissions/2021/home_affairs_draft_critical_infrastructure_assets_definition_rules_13may.pdf; Submission to Home Affairs (November 2020), Link: https://www.aigroup.com.au/globalassets/news/submissions/2020/home_affairs_critical_infrastructure_security_reforms_exposure_draft_bill_nov2020.pdf; Submission to Home Affairs (September 2020), Link: https://www.aigroup.com.au/globalassets/news/submissions/2020/dept_home_affairs_critical_infrastructure_security_reforms_sept2020.pdf.

[14] These are examples of matters that we raised (amongst others) in our submission to the PJCIS in February 2021 concerning the uncertainty around the scope of these reforms. Please refer to our February 2021 submission for further details.

which assets would be covered by the legislation. Consideration should be given to retaining the requirement of "wholly or primarily" as part of these definitions.

Ai Group recommendation: Further clarity be provided on the entities covered and not covered in these reforms.

2.2 Potential duplication of existing requirements

We acknowledge an intent of the Bill is to not duplicate existing regulations. As previously stated, if the reforms are co-designed well, it can help to avoid such a scenario, as well as lead to other mutually positive outcomes.

Amongst various suggestions and recommendations made in our previous submissions, we proposed a solution where a thorough gap analysis and assessment could be undertaken of the proposed obligations against existing obligations across the various sectors. This should assist the various sectors covered in this Bill, as well as for those that operate across sectors. Such a gap analysis may also 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. Once these are clarified for the various sectors, further consideration could be given to businesses that operate across sectors. 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 example, the issue of duplicated arrangements could arise with respect to the proposed PSO in the Bill for Risk Management Program should there be existing arrangements or practices in place for a given sector or entity. More generally, it could arise with any obligation that was introduced under the SLACI Act and other obligations proposed in this latest Bill.

Ai Group recommendation: A thorough gap analysis and assessment be undertaken on the proposed obligations in the SLACIP Bill against existing obligations across the various sectors.

2.3 Enhanced Cyber Security Obligations

We previously expressed our support in principle for 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 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".[15] 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.

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.

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.[16] 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

[15] Explanatory Document to SLACIP Bill, p. 16.
[16] Explanatory Document to SLACIP Bill, pp. 19-20.

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.

We discuss some of the above matters in further detail below.

2.3.1 Non-regulatory options

With respect to non-regulatory approaches, the value of education, communication and engagement activities should not be underestimated, especially in building trust and facilitating genuine collaboration between governments and industry. This was previously acknowledged in the Explanatory Memorandum to the SLACI Bill 2020, 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".[17]

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 proposed obligations. 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.

Ai Group recommendation: Non-regulatory options be considered as alternatives to the proposed obligations under the SLACIP Bill.

2.3.2 Mutual obligations

Mutual obligations should be clarified between the relevant government authorities (i.e. ASD) and entity under the proposed obligations such as the ECSO and information sharing requirements.

For example, the Explanatory Document to the Bill indicates that the ECSO "would support the bi directional sharing of threat information to provide industry with a more mature understanding of emerging cyber security threats, and the capability to reduce the risks of a significant cyber attack against Australia's most critical assets".[18]

However, it is not clear if the intention of these obligations is reflected in legislation. If such obligations were to be required of an entity, it would be helpful to understand how the ASD will assist the entity following the entity undertaking an obligation. This would help to provide transparency and establish a genuine bilateral relationship of trust between the ASD and 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 under the Risk Management Program obligation. 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 other obligations 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?

[17] Explanatory Memorandum to SLACI Bill 2020, para 7.
[18] Explanatory Document to the SLACIP Bill, p. 6.

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 and authorities such as Emergency Management Australia, Geoscience Australia and Bureau of Meteorology for other types of threats.

Ai Group 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.***

2.3.3 Civil penalties

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.

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

2.4 Safeguards and oversight

A significant concern that we have previously raised related to the Government's powers in the SLACI Bill 2020 that proposed to exempt ministerial authorisations and administrative decisions made under these powers from being subject to judicial review. Some reasons previously provided in the Explanatory Memorandum to that Bill were that seeking exemption from judicial review "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 to the SLACI Bill 2020 suggested 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 has offered a satisfactory level of assurance to industry. We also consider that the obligations arising from the SLACI Act and SLACIP Bill should be subject to adequate independent oversight while also addressing the Government's needs. For example, similar considerations were given during the TOLA Act Review by the Independent National Security Legislation Monitor (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 suggested that it could also be a relevant approach for consideration in these critical infrastructure security 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. Supporting this, we note that the PJCIS contemplated in its Advisory Report of the need to review the legislation at some point (particularly recommendations 8 and 14) and further consideration be given to independent oversight.[19]

[19] PJCIS Advisory Report to the SLACI Bill 2020, pp. xviii-xx, 77-78.

In addition to the last resort powers under the SLACI Act, 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.

Separately, entities impacted by Government directions, particularly under the ECSO, should be afforded appropriate safeguards by the legislation, including:

- Clarity about liability and indemnification e.g. in the case of loss of life, property damage or breach of contract caused as a consequence of following a Government direction; and

- Ensuring that actions (or inaction) at the direction of Government cannot be used to exclude an insurer's liability under a policy of insurance e.g. cyber insurance.

Ai Group 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.***

- ***Clarity be provided about the impact on liability and insurance as a consequence of following Government directions.***

2.5 Regulatory impact assessment

The Explanatory Memorandum to the SLACI Bill 2020 included some form of cost-benefit assessment with respect to the ECSO. We considered this inferred that the costs were 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."

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 clarifying rules) that 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 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 clarifying 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.

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, including for an expanded range of businesses. For example, businesses may need to increase or upskill personnel capability to help them properly meet new regulatory obligations.[20] This will be especially important for companies that are not traditionally subject

[20] 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

to these types of reforms, which will need as much assistance as possible to ensure that they are properly accounted for. It is important to note that this is not necessarily about just providing funding support for large technology businesses, but about SMEs and wider industry that may be captured under these requirements with practical uplift support.

- 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 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 these other initiatives, this will need to be publicly accounted for. This 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 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 and impact on company investment risk credit rating of entities subject to the new laws that may be perceived to be overly intrusive.

- We are cautious with proposals relating to regulatory reforms, without a proper assessment of whether the relevant government departments, agencies and authorities have the sufficient resources funded by Government to execute its functions. For example, there may be adequate regulations in place, but the regulator may have insufficient resources. If the regulator were to be provided with sufficient resources that contributed to addressing an identified issue, then this suggests that the regulations in place are sufficient. We suggest this would be a more prudent step rather than immediately resorting to legislative reforms associated with regulation in the first instance.

Ai Group recommendation: Government undertakes a proper quantitative cost-benefit assessment for the proposed reforms prior to making legislation.

If you would like clarification about this submission, please do not hesitate to contact me or Charles Hoang (Lead Adviser – Industry Development and Defence Industry Policy, [redacted]).

Yours sincerely,

Louise McGrath
Head of Industry Development and Policy

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.