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

17 March 2022

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

Dear Senator Paterson

SUPPLEMENTARY SUBMISSION TO REVIEW OF THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE PROTECTION) BILL 2022

The Australian Industry Group (Ai Group) would like to thank the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for providing us with the opportunity to appear at the public hearing on 16 March 2022 as part of its review into the Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (SLACIP Bill 2022). The PJCIS continues to play a critical role in reviewing this Bill and ensuring that relevant matters are properly considered.

During our session at the public hearing, the PJCIS expressed a specific interest regarding the defence industry's perspective about this Bill, which we briefly touched upon. For completeness, we would like to refer the PJCIS to our previous comments made in our supplementary submission to the PJCIS on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (SLACI Bill 2020) regarding the defence industry, as we consider these comments remain pertinent to the SLACIP Bill 2022.[1]

Finally, a particular matter that arose during the public hearing related to a discussion on the proposed obligation under section 30DJ of the SLACIP Bill 2022 where the Secretary may require installation of system information software. While we offered general comments during the hearing, we would like to offer additional comments to assist the PJCIS in its deliberations.

1. Secretary may require installation of system information software

We note that section 30DJ of the SLACIP Bill 2022 would empower the Home Affairs Secretary who "may require a relevant entity for a system of national significance to install and maintain a specified computer program in limited circumstances".[2] Reasons provided in the associated Explanatory Memorandum include: providing government with oversight of cyber security risks where an entity lacks capacity to provide system information (for example, it would require a costly reform to their system); enabling the sharing of system information from the entity to Government; and informing the ASD on an enhanced cyber threat picture so it can develop appropriate mitigations and advice for the entity. This obligation is attached with a civil penalty for non-compliance under section 30DM (Compliance with system information software notice).

We note that this concept was originally proposed in the SLACI Bill 2020 and subsequently carried through to the SLACIP Bill 2022. We previously commented about this and would like to reiterate our views.

While we support in principle information threat sharing with Government, there is a risk that this particular requirement (under proposed section 30DJ) may be regarded as 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

[1] Ai Group supplementary submission to PJCIS, Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (No 41.1, 26 July 2021), https://www.aph.gov.au/DocumentStore.ashx?id=9a17320c-05e0-450b-adb4-0389d69bf927&subId=701595.
[2] Explanatory Memorandum to the SLACIP Bill 2022, p. 98, Para 505, https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6833.

Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018 (Cth) (TOLA Act) being repeated in this latest Bill.

There are also concerns about how that information is handled, stored, shared etc. This is especially concerning for businesses where that information is considered to be sensitive or classified. If such information were not properly managed by the relevant government body (albeit done in good faith), this presents a risk for the entity.

2. Alternative approach to section 30DJ

We understand that an alternative approach posed during the public hearing was whether entities would be comfortable if they were given the responsibility of installing their own system software that would produce system information and provide this to the ASD on request i.e. system information software designed, installed and operated by entities (instead of being designed, installed and operated by government). A perceived benefit may be to avoid concerns arising from direct government intervention.

On its face, this proposed alternative approach may have merit for further consideration and be preferred over proposed section 30DJ.

However, we are cautious about potential practical problems that this approach might present to entities. For example, consideration needs to be given as to whether there would be a negative impact on an entity's trade activities and obligations (e.g. export control requirements), extent of costs to entities to implement such a system, and liabilities arising from negative unintended consequences. And if entities were compelled to provide system information to government, there will be ongoing concerns about the type of requested information and how it will be adequately protected.

Therefore, should this alternative approach be considered further, we strongly recommend that it needs to be closely worked through between government and affected entities to better understand the required information and regulatory impact (including costs), and ensure appropriate safeguards are put in place.

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