The Australian Industry Group
Level 2, 441 St Kilda Road
Melbourne VIC 3004
PO Box 7622
Melbourne VIC 3004
Australia
ABN 76 369 958 788

26 July 2021

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) BILL 2020

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 8 July 2021 as part of its review into the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Bill). The PJCIS plays a critical role in reviewing this Bill and ensuring that relevant matters are properly considered.

Ai Group's members are businesses of all sizes and many sectors across Australia, including the defence industry. 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.

In this regard, we welcome our continued inclusion in further consultations, along with relevant members covering a wide range of sectors that may be captured by these reforms, and the opportunity to work closely with the Department of Home Affairs (Home Affairs), PJCIS and other relevant government departments and agencies on these reforms.

During our session at the public hearing, the PJCIS expressed a specific interest regarding the defence industry's perspective about this Bill and we briefly shared our opinion. To assist the PJCIS in its deliberations, we would like to offer additional information to elaborate on our comments and provide further context.

1. About the Defence Council

Ai Group has many members in the defence industry and we also run a separate Defence Council which plays its part in supporting Australia's national security objectives.

The Ai Group Defence Council is the peak national representative body for the Australian defence industry. The role of the Defence Council is to address significant issues that impact the defence industry. It provides a forum for building and developing the shared interests of the industry through its National Executive and Working Groups which inform policy development, develop initiatives, and promote the shared interests of the Department of Defence (Defence) and industry.

It is fair to say that the defence industry has a strong relationship with Defence and other Government agencies, given the nature of its work. To facilitate this further, the Defence Council brings Government, Defence and defence industry together for the benefit of national security and the growth and development of the national defence industry.

2. Security requirements for the defence industry

Defence and associated industry are prime targets for hostile foreign governments, as well as having to deal with cyber crime, human error and insider threats. Defence and industry therefore take security very seriously.

There are various legislations, regulations and policies that guide defence industry security including the following:

- Australian Government Information Security Manual (ISM);
- Australian Government Protective Security Policy Framework (PSPF);
- *Australian Human Rights Commission Act 1986* (Cth);
- *Customs Act 1901* (Cth);
- Defence and Strategic Goods List (DSGL);
- Defence Security Principles Framework (DSPF);
- Defense Federal Acquisition Regulation Supplement (DFARS) and Federal Acquisition Regulation (FAR);
- European Union's General Data Protection Regulation (EU GDPR);
- International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR);
- *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) and *Criminal Code Act 1995* (Cth); and
- *Privacy Act 1988* (Cth).

There is also a range of Government, Defence and other organisations that have important roles and responsibilities in relation to Defence and defence industry security. These include:

- Australian Cyber Security Centre (ACSC);
- Australian Government Security Vetting Agency (AGSVA);
- Australian Security Intelligence Organisation (ASIO);
- Centre for Defence Industry Capability (CDIC);
- Chief Information Office Group (CIOG);
- Defence Industry Security Office (DISO); and
- Defence Security and Vetting Service (DS&VS).

During the public hearing, we mentioned the Defence Industry Security Program (DISP) as an example (also previously mentioned in our February submission). Defence encourages all organisations interested in working with Defence to consider applying for DISP membership and, in some cases, it is mandatory to join the program if they are doing sensitive or classified work. The DISP offers substantial benefits to Defence and industry in streamlining security services and protecting Defence information and assets, as well as industry's intellectual property. The DS&VS is responsible for managing the DISP.[1]

Any Australian business can apply for DISP membership. To successfully become a DISP member, they will need to meet the eligibility and suitability requirements outlined in Control 16.1 of the DSPF.[2] Control 16.1 of the DSPF relates specifically to the DISP. It provides principles, controls and instructions to support defence industry to understand and manage security risks when engaging with Defence.[3]

Within this security framework, standards play an important role. In the case of the DISP, DISP members must meet various requirements including meeting one of the following cyber security standards:

- Top 4 requirements of the ASD Essential 8:
    - application control;
    - patch applications;
    - restrict administrative privileges; and
    - patch operating systems;
- ISO/IEC 27001 and 27002;
- NIST SP 800-171 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (US ITAR requirement); and
- Def Stan 05-138 *Cyber security for defence suppliers*.

[1] A revised DISP was launched on 9 April 2019 to meet the requirements of a modern Defence organisation, representing a fundamental change in approach to industry security.
[2] The DSPF provides principles, controls and instructions to support Defence personnel, contractors, consultants and outsourced service providers, to manage security risks.
[3] See website for more information: https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf; https://www1.defence.gov.au/security/industry/eligibility.

There are also other standards, not limited to cyber security, that DISP members must meet such as AS 4811-2006 *Employment Screening* which relates to personnel security. This is not an exhaustive list of standards that are relevant to defence industry security; it highlights the range of existing security standards applicable to the defence sector.

To assist companies wishing to work in Defence, our Defence Council's Security Working Group in cooperation with Defence and other Government agencies including the ACSC, developed a guide *Working Securely with Defence* which was released in February this year. The purpose of this guide is to:

- provide the pathway for businesses to become eligible for classified and sensitive Defence work through participation in the DISP;
- provide practical guidance, tools and expert advice to help protect Australian organisations from a range of security threats;
- help build the competitiveness and security resilience of the defence industry sector through good security practices; and
- assure international investors and partners of industry's commitment to Defence security.

The guide includes a range of industry tips, case studies, links to relevant resources, assistance, contacts and templates. With input from Defence and industry, all this information has been designed to assist businesses in putting together their DISP applications.[4]

3. Scope of the Bill

Our previous submission raised various matters for the PJCIS's consideration, including with respect to the scope of the Bill, consultation process, and duplication of existing arrangements or requirements. For the purposes of this submission, we elaborate further on these specific points, taking into consideration the context above.

Potential breadth of companies covered

Our previous submissions discussed our concerns regarding the reforms' potential wide coverage that could affect many businesses. It is fair to say that many engaged sectors and businesses are seeking to better understand the scope of the Bill and its impact on their particular businesses. The Bill is explicitly targeted at 11 critical infrastructure sectors that have been identified to be subject to the Exposure Draft Bill including the defence sector; it also has a potentially wider scope that may encompass many companies.

Notwithstanding the comprehensive security arrangements for the defence industry as noted above, it is also important to appreciate the diverse nature of defence businesses, as well as other businesses that form part of the defence industry supply chain. And this is not only limited to the defence industry.

More generally, 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 (but not limited to) suppliers, manufacturers and "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.[5]

The scope 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 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

[4] The above information has been extracted from the guide and is only a snapshot of relevant security considerations for those interested in engaging in Defence work. A copy of our guide can be found here: https://www.aigroup.com.au/business-services/industrysectors/defence/defence-industry-security-program/.

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

requirements and assist relevant Government agencies (including regulatory bodies) in understanding their roles should such a Bill be implemented.

However, 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.

Consultation process considerations

Generally, we have welcomed the consultative approach that Home Affairs has undertaken in holding virtual town halls and workshops.

However, as previously stated, we consider that the Bill has not addressed various areas of uncertainty and it was premature to have this Bill tabled into Parliament in December last year.

We acknowledge that Home Affairs has been consulting through workshops concurrently to this Bill on sector specific rules with the electricity and gas sectors being the first sectors. This has now been followed by the data storage and processing, and water sectors. However, other identified sectors in the Bill are yet to be considered. Home Affairs has also this year consulted on generic governance rules, and critical asset definitions and rules. These concurrent consultations have been undertaken in anticipation of legislation being passed through Parliament.

Our preference would have been for these consultations, especially on sector specific requirements, to have occurred prior to the Bill having been 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 have been many relevant and important questions and ideas raised by the PJCIS and stakeholders during the public hearing about the Bill – this may be due to issues and options not having been properly worked through before it was tabled into Parliament.

Given these parallel consultations, there may also be confusion for all parties (including policy makers and stakeholders) regarding the order of reforms. For instance, should changes arise from the PJCIS' review, this could impact on Home Affairs' consultation and stakeholders may need to be consulted again. In our submission to Home Affairs on its Draft Critical Infrastructure Asset Definition Rules paper consultation in May, we suggested that there should be time allowed for the PJCIS review to be completed before other related consultations arising from the Bill commence.

There is also the matter of interrelated reforms and activities that need to be accounted for; some of which we have raised in our February submission.

Addressing 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.

In the case of the defence industry with respect to this Bill, we discussed an example in our previous submission that concerned the sector. The Explanatory Memorandum acknowledged the existing non-regulatory risk management framework and obligation under the DISP, managed by Defence in partnership with industry. While the Explanatory Memorandum appeared to deem that the existing Defence security mechanisms under the DISP were appropriate insofar as it related to the Positive Security Obligation (PSO), it was not clear whether this extended to the application of the Enhanced Cyber Security Obligation (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 were designated as systems of national significance) and Government Assistance measures would still apply to the defence sector but this appeared 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' acceptance of the DISP. With this no longer explicitly mentioned in the Explanatory Memorandum, it was unclear whether these proposed obligations would still apply to the defence sector.

Amongst various suggestions and recommendations made in our previous submission, we proposed a possible solution where a thorough gap analysis and assessment could be undertaken of the proposed obligations against existing obligations across the various sectors. This should not only

assist the defence industry but also other 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.

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