



The Australian Industry Group Submission to Joint Standing Committee on Foreign Affairs, Defence and Trade

Defence Industry Security Program
November 2022

October 2022



Introduction

The Ai Group Defence Council welcomes the opportunity to provide a submission to the Joint Standing Committee on Foreign Affairs, Defence and Trade in relation to the inquiry into matters contained within the *Auditor-General's Report No. 4 (2021-22) Defence's Contract Administration – Defence Industry Security Program*.

The Ai Group Defence Council is the peak national representative body for the Australian defence industry. We bring Government, Defence and defence industry together for the benefit of national security and the development of the defence industry, as well as providing trusted advice to a wide range of Defence and industry stakeholders.

The Ai Group Defence Council convenes working groups with the Department of Defence, industry members and other stakeholders across a range of important policy areas, including security.

The Defence Council Security Working Group works closely with the Department of Defence to provide information exchange opportunities, and provide trusted advice and input to policy positions for the benefit of both Defence and industry. We would like to thank the industry members of the Security Working Group who have helped inform the views in this submission.

The Defence Industry Security Program (DISP) is a critical underpinning for the Australian defence industry and national security more broadly, as well as an enabler of industry as a fundamental input to capability. The Australian defence industry relies heavily on the program and its administration to build Australian capability and further develop the Defence and industry partnership.

Overall, feedback to us is that there have been many positive changes and benefits since the expansion and changes to the DISP in April 2019.

However, we have also received feedback that significant reform is still required to make the operations of the DISP program more efficient and effective. Responses to us have emphasised the importance of appropriate skill and experience levels in Defence in administering the DISP program, as well as the importance of extensive consultation on policy issues that affect defence industry. A further theme noted the importance of moving from a 'compliance' mindset to a risk management approach in accordance with the principles of the Defence Security Principles Framework (DSPF).

Background and context

The *Auditor-General's Report No. 4 (2021-22) Defence's Contract Administration – Defence Industry Security Program* was released in September 2021 and contained a range of findings and recommendations.

The Report found that:

- Defence's administration of contractual obligations relating to the DISP is partially effective.
- Defence's arrangements for administering contracted DISP requirements are partially fit for purpose.



- Defence has not established fit for purpose arrangements to monitor compliance with contracted DISP requirements.
- Defence has not established effective arrangements to manage identified noncompliance with contracted DISP requirements.

There were six recommendations to Defence aimed at: improving contracting templates, training and support for contract managers; improving DISP assurance processes and supporting documentation; and establishing a documented framework for managing non-compliance with contracted DISP requirements. Defence agreed to the recommendations.

Key themes

In April 2019 important changes were made to the Defence Industry Security Program that were welcomed by industry. In particular, DISP membership is now open to any Australian entity interested in working with Defence, rather than requiring a company to already have a contract with Defence. In addition, there have been benefits from expanding the program so there are now different levels of DISP membership based on security classifications.

Defence has also responded positively to the requirement for additional resources to assist with the earlier backlog of applications for DISP. It is understood that, due to this application of resources, Defence has made significant progress with speeding up the assessment of applications.

Defence industry also appreciates the efforts that are being made with regard to industry engagement. Defence has held a series of industry roundtables, and it is understood these will continue in 2023. Ai Group commends Defence for the outreach program, and we appreciate the engagement and support that we receive through the Ai Group Defence Council Security Working Group. The Security Working Group is well attended by senior Defence and industry and is an effective mechanism for information exchange and input to policy development.

We understand that Defence has continued to develop the contracting suite to implement DISP requirements and mature the contract administration aspects of DISP.

While significant progress has been made, there are still areas where improvements are warranted to increase the effectiveness and efficiency of the DISP program.

- 1. Risk management versus compliance approach.** We received feedback that a move towards risk management in line with the requirements of the Defence Security Principles Framework would create a more effective approach to defence industry security and managing risk. This approach would also reflect the principles of the Commonwealth Protective Security Policy Framework. A move to a more mature model of risk management for security related risks, rather than “templated” compliance requirements will be more efficient and effective. It will also be of assistance to those companies who operate in other sectors of mandated action in the designated areas of critical infrastructure and systems of national significance.
 - The increasing critical infrastructure and cybersecurity challenges will see the need to bring into the Defence sector non-traditional industry participants where engagement will necessitate a risk-based approach. Further, movement to a risk-based approach enables Defence and industry to focus on security in areas of critical importance avoiding a ‘one-size-fits-all’ methodology.



2. **Education, skill sets and experience levels in the Defence workforce.** Feedback to us noted the importance of appropriate levels of skills and experience in the Defence workforce. Specifically, it was noted it can be difficult to gain clear and consistent guidance on particular topics. This issue requires recognition of the complexity of defence industry security, and the deep skill set and experience required to build a workforce that can implement the DISP effectively. We suggest that Defence security managers and leaders should not just be public service 'generalists' but have deep knowledge and proficiency in security related matters. We recommend that Defence review and develop a strong education and training program, and a workforce strategy to meet the requirements of the DISP.
3. **Industry consultation processes on policy and guidance.** Ai Group commends Defence on the engagement and outreach programs by Defence security teams. The development of the 2019 changes to the DISP was an example of industry consultation and co-design to ensure industry was heard in relation to the impact of the changes to policy. Since then, our view is that industry consultation could be improved in terms of the depth and breadth of engagement where policy changes will impact industry. We are particularly focussed on helping to ensure the operating environment does not become overly complicated and a barrier to SME engagement.
4. **Strengthening of DISP processes and information exchange.** We suggest that improvements can be made to DISP processes and approaches that would strengthen the DISP community and compliance, as well as provide additional efficiencies. For example, it would be useful to understand the DISP status of other members within the DISP community. We are acutely aware of the security issues surrounding this suggestion – industry is of the view that there are sensible workarounds. Another area where the program could be strengthened relates to additional resourcing and processes to provide security assurance.
5. **Subcontractors and AS4811:2022 pre-employment screening.** There are areas that require further engagement between industry and Defence, in particular the process of engagement and management of subcontractors and the requirements for AS4811:2022 pre-employment screening. Some companies have recruitment and personnel management practices reflecting the standard and apply it in conduct vetting for employment to the requirements of the base level clearance. Consideration should be given to authorised DISP companies to conduct their own clearances rather than having to duplicate the process. There would be considerable savings in time and resources.

The Protective Security Policy Framework & DSPF were written for government agencies and departments, and while there are some areas/sections that specifically relate to DISP membership, the remainder of the framework is still very Government agency specific. Compliance around pre-employment screening (AS4811:2022) is difficult for existing staff who may have held a clearance for the last 15 years and revalidation is triggered (they have not strictly speaking undergone AS4811:2022 process).

The above personnel assurance matters would be resolvable with appropriate "grand parenting provisions" and a review of current guidance to develop a more streamlined approach.



Recommendations

Ai Group recommends that the DISP be strengthened and improved by:

- a. developing the DISP away from a compliance model to a mature risk management approach in accordance with the Defence Security Principles Framework;
- b. implementing a new strategy for training, education, workforce and skill development for the Defence security workforce;
- c. strengthening industry consultation and engagement processes to provide meaningful opportunities to provide input into Defence security policy; and
- d. strengthening the integrity of the DISP through additional assurance measures and information exchange within the Defence community. This should include a review of the processes around subcontractors and pre-employment screening.

We welcome this opportunity to provide our views to the Joint Standing Committee on Foreign Affairs, Defence and Trade on the DISP and the Report. Overall, the changes to the DISP have been positive and Defence has worked with industry to improve implementation. However, there are a range of areas where implementation of the DISP could be strengthened to boost Defence and industry's overall security resilience.

We would be very happy to discuss this submission further as required.

© Ai Group, 2022

The copyright in this work is owned by the publisher, Ai Group Limited, Level 2/441 St Kilda Road, Melbourne VIC 3004. All rights reserved. No part of this work may be reproduced or copied in any form or by any means (graphic, electronic or mechanical) without the written permission of the publisher.

