OFFICIAL

Auditor-General for Australia

Australian National Audit Office

13 July 2023

Senator Raff Ciccone
Foreign Affairs, Defence and Trade Legislation Committee
By Email: fadt.sen@aph.gov.au

Dear Senator Raff Ciccone

Performance of the Department of Defence in supporting the capability and capacity of Australia's defence industry

The Australian National Audit Office (ANAO) published the following performance audit reports that you may find relevant to the above review.

- Auditor-General Report No. 6 (2020-21) *Design and Implementation of the Defence Export Strategy*
- Auditor-Generals Report No. 4 (2021-22) *Defence's Contract Administration — Defence Industry Security Program*

Information about what the audits assessed, concluded and recommended is attached. The audit reports are available online at www.anao.gov.au.

Should the Committee require further information in relation to these matters, my office would be pleased to provide you with a briefing at a time convenient to you or appear as a witness at a hearing.

Yours sincerely

Grant Hehir

GPO Box 707, Canberra
ACT 2601
38 Sydney Avenue, Forrest
ACT 2603

Auditor-General Report No.6 (2020-21) *Design and implementation of the Defence Export Strategy*

Background

1. The Joint Standing Committee on Foreign Affairs, Defence and Trade recommended in November 2015 that the Australian Government develop a 'defence exports strategy' to assist in reducing barriers to defence exports.[1] The Australian Government provided in principle agreement to this recommendation on 1 September 2016. The Australian Government's Defence Export Strategy (the strategy) was launched on 29 January 2018

2. The strategy sets out a strategic goal and five objectives for the development of defence exports by 2028. The strategy includes 26 initiatives that 'the Government will deliver to help achieve the Strategic Goal and the Objectives of the Strategy'. [2]Together, the policies and initiatives in the strategy are described as a 'new defence export system'. [3]The strategy states that the initiatives will be implemented in two phases, with Phase 1 to be implemented by the end of 2018, and Phase 2 to be implemented by the end of 2019.[4]

Rationale for undertaking the audit

3. The Australian Government has stated that 'a strong, resilient and internationally competitive Australian defence industry is essential to our national security.'[5] The government's Defence Export Strategy is intended to implement key recommendations made by the Parliament's Joint Standing Committee on Foreign Affairs, Defence and Trade in its 2015 report on Australian defence industry and exports, and sets out an ambitious policy agenda to be delivered by 2028, including establishing Australia as one of the top ten global defence exporters. This audit provides the Parliament with independent assurance on Defence's design process for the strategy and its implementation to date, with a particular focus on the initiatives government expected to be delivered by the end of 2018 under Phase 1 of the strategy, and by the end of 2019 under Phase 2.

Audit objective and criteria

4. The objective of the audit is to assess the effectiveness of Defence's design process and implementation to date of the Defence Export Strategy.

---

[1] Joint Standing Committee on Foreign Affairs, Defence and Trade, *Principles and practice – Australian defence industry and exports,* November 2015. Barriers to entry that the committee identified were: international market competition and distortions caused by protectionist measures, industry challenges, assistance needed with sponsorships and advocacy and assistance needed selling to the ADF to build business credibility. Available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/Defence_Industry_Exports/Report [accessed 18 May 2020].

[2] Department of Defence, *Defence Export Strategy,* 2018, p. 15.

[3] Ibid., p. 16.

[4] Ibid., p. 76.

[5] Ibid., p. 4.

5. To form a conclusion against the audit objective, the ANAO adopted the following high level criteria:

- Did Defence help inform the design of the export strategy with sound and timely policy advice?
- Has Defence established appropriate planning and governance arrangements to support implementation of the strategy?
- Has Defence delivered the phase one and two initiatives set out in the strategy on time and on budget?
- Has Defence established effective arrangements to monitor and report on the implementation of the initiatives under the strategy and achievement of defined objectives?

Conclusion

6. Defence's design and implementation to date of the Defence Export Strategy has been partially effective.

7. The design process was largely effective. In designing the strategy Defence consulted with relevant stakeholders, but not all elements of the strategy had a firm evidentiary basis. Defence did not adequately draw the attention of decision-makers to key risks it had identified. Defence was responsive to government's initial decisions and directions but was unable to meet the timeframes set by the Minister for finalising the strategy.

8. Strategy implementation has been partially effective. While Defence established fit-for-purpose governance arrangements, planning arrangements were not established to appropriately support implementation of the strategy initiatives on time and on budget. Defence did not deliver all Phase 1 and Phase 2 initiatives in accordance with strategy timeframes and has not tracked expenditures relating to the strategy as a whole.

Supporting Findings

9. Defence provided government with advice on the approach and rationale for developing a strategy, based on its consultation with government entities and industry. The approach to strategy development agreed by the Minister for Defence Industry was not fully addressed by Defence, with baseline data for defence exports not identified. Options for elements to be included in the strategy were discussed within Defence, the Minister's office was provided drafts for consideration, and the final strategy was presented to the Minister for approval. Available evidence indicates that Defence responded to government's initial decisions and directions in a timely manner but did not meet the expectation of the Minister in terms of finalising the strategy by September 2017.

10. The strategy objectives and initiatives developed by Defence were largely supported by research and consultation but were not informed by robust defence export data. The inclusion of objective five — growing Australia's defence industry to become a top ten global defence exporter — reflects an announcement by the Minister for Defence Industry and was not supported by analysis or data. Defence did not clearly map how the strategy initiatives would contribute to the achievement of strategy objectives.

11. Defence considered key risks and mitigation strategies during the strategy's development, such as maintaining a strong export controls system and ensuring a focus on Defence capability outcomes. While Defence provided adequate detail to Defence Ministers, it did not provide all Ministers with adequate detail on risk and implementation challenges to more fully inform their decision-making.

12. Defence has established and implemented fit-for-purpose governance, co-ordination and stakeholder engagement arrangements to support delivery of the strategy. Roles and responsibilities for the strategy's governance and implementation have been clearly identified. Defence has established co-ordination mechanisms within government and arrangements to engage with relevant external stakeholders. Stakeholders interviewed by the ANAO expressed a view that these mechanisms had improved collaboration across government for defence exports.

13. Defence prepared a draft implementation plan which addressed key implementation issues including risks, delivery milestones, roles and responsibilities. However, the plan was not finalised or used and implementation was managed through business-as-usual mechanisms. Defence advised that tools such as checklists and 'road maps' were utilised instead to support implementation.

14. Of the eight phase one key milestones, Defence has delivered two initiatives on time, delivered four initiatives between five days and six months late, and not yet completed two initiatives. Defence does not monitor the phase one budget at an initiative level.

15. Of the three phase two initiatives, one initiative was not delivered on time. It is not possible to assess the timeliness for the remaining two initiatives because the strategy does not set out what completion of the initiative would involve. Defence does not monitor the phase two budget at an initiative level.

16. Of the five other key initiatives, Defence has made progress delivering four of these initiatives. The market intelligence capability is yet to be delivered.

17. Defence has not established a performance framework or effective reporting arrangements to measure progress towards achieving the strategy's overarching goal and objectives. As of June 2020, Defence had not established baseline data for defence exports or a methodology for measuring defence exports. At the initiative level, a framework to assess the progress of strategy initiatives has been developed and mechanisms have been implemented for two initiatives to assess achievements and consider lessons learned from their specific activities.

18. There is limited reporting on progress in delivering the strategy to the Minister and Defence senior leaders, to demonstrate that the strategy is contributing to the outcomes that government expects. There is no reporting or publicly available information on Defence's achievement towards strategy objectives, although there has been public reporting on the progress of some strategy initiatives.

Recommendation

Recommendation No.1

That Defence extend the Defence Export Strategy's performance framework and develop an evaluation framework to measure and report on the achievement of the strategy's overarching goal and specified objectives.

Auditor-Generals Report No.4 (2021-22) *Defence's Contract Administration – Defence Industry Security Program*

Background

1. The Department of Defence (Defence) engages with industry to develop, deliver and sustain Australian Defence Force (ADF) capability and to meet its business requirements. As at 24 March 2021, Defence reported that it had 16,503 active contracts with a total commitment of $202.4 billion.[1] These contracts were for a range of goods and services including: platforms and sustainment services; estate management; IT systems and support; inventory; research and development; and management consultancies.

2. The Defence Industry Security Program (DISP) is a long running program in Defence spanning several decades. The Defence Security Principles Framework (DSPF) sets out the security requirements that industry entities must meet to obtain and maintain DISP membership. The DSPF states that:

> Industry Entities (Entities) must hold an appropriate level of Defence Industry Security Program (DISP) membership when working on classified information or assets[2] ; storing or transporting Defence weapons or explosive ordnance; providing security services for Defence bases and facilities; or as a result of a Defence business requirement specified in a contract.[3]

3. The DISP aims to support Australian businesses to understand and meet their security obligations when engaging in Defence projects, contracts and tenders. In April 2019, the Minister for Defence Industry announced that DISP membership would be opened to any Australian entity interested in working with Defence, rather than requiring a company to already have a contract with Defence. In addition to expanding the program, different levels of DISP membership, based on security classifications, were introduced.

Rationale for undertaking the audit

4. Defence has stated that the DISP 'is essentially security vetting for Australian businesses'.[4] The DISP is a long-running program intended to support industry entities to understand and meet their security obligations when engaging in Defence projects, contracts and tenders. During its inquiry into Australian Government Security Arrangements, the Parliament's Joint Committee of Public Accounts and Audit (JCPAA) questioned Defence about the compliance mechanisms Defence had in place to provide assurance that industry entities contracted to Defence are meeting their security obligations.[5] In its report on that inquiry, the JCPAA noted that: 'Defence was not able to provide the level of confidence or assurance that the Committee required'.[6] This audit provides the Parliament with

---

[1] These figures were obtained from AusTender data provided to the ANAO by the Department of Finance. The figures only include contracts above the reporting threshold of $10,000. There is a 'lag time' of 42 days for AusTender data as entities have that amount of time from entering into (or amending) a contract above the reporting threshold before they have to report it on AusTender. The dataset provided by AusTender may not capture contracts entered into over the last 42 days if they have not been reported on AusTender. Further, information contained in AusTender is self-reported by entities, so the completeness and accuracy of data is dependent on them.

[2] ANAO comment: under Defence's current DISP arrangements, this means information or assets with a national security classification of PROTECTED or above.

[3] Department of Defence, *Defence Security Principles Framework (DSPF) Defence Industry Security Program*, available from https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL-Principle-16-Control-16.pdf [accessed 19 July 2021]. See Control 16.1, p. 1

[4] Department of Defence, Defence Industry Security Program website, www1.defence.gov.au/security/industry [accessed 9 March 2021].

[5] Joint Committee of Public Accounts and Audit, *Report No.479: Australian Government Security Arrangements: Personnel Security and Domestic Passenger Screening - Inquiry Based on Auditor-General's reports 38 and 43 (2017-18).* https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/PersonnelSecurity [accessed 13 July 2021].

[6] Ibid., p. 24.

independent assurance of the effectiveness of Defence's arrangements to manage security risks when procuring goods and services from industry through its implementation of the DISP.

Audit objective and criteria

5. The objective of the audit was to examine the effectiveness of Defence's administration of contractual obligations relating to the Defence Industry Security Program (DISP).

6. To form a conclusion against the audit objective, the ANAO adopted the following high-level criteria:

- Has Defence established fit for purpose arrangements for administering contracted DISP requirements?
- Has Defence established and implemented fit for purpose arrangements to monitor compliance with contracted DISP requirements?
- Has Defence managed non-compliance with contracted DISP requirements?

Conclusion

7. Defence's administration of contractual obligations relating to the Defence Industry Security Program (DISP) is partially effective. While Defence has established a framework and communication arrangements for DISP, the administration of the DISP does not enable Defence to gain assurance that the program is effective.

8. Defence's arrangements for administering contracted DISP requirements are partially fit for purpose. Support for Defence contract managers and industry entities regarding DISP has been partially effective, with Defence only establishing arrangements to manage the backlog of DISP applications in January 2021.

9. Defence has not established fit for purpose arrangements to monitor compliance with contracted DISP requirements. In particular:

- Defence has not fully implemented the compliance and assurance framework identified in the Defence Security Principles Framework;
- Defence does not know which of its active contracts should, or do, require the contracted entity to have DISP membership, a situation which limits the effectiveness of DISP as a security control; and
- Defence contract managers are not provided with relevant information to help them monitor and manage contractor compliance with contracted DISP requirements.

10. Defence has not established effective arrangements to manage identified non-compliance with contracted DISP requirements. In particular, Defence has not established an appropriate.

Supporting findings

Administering contracted DISP requirements

11. Defence has developed a framework that is largely effective in defining DISP requirements. While DISP requirements are clearly defined in the security policy, there is scope for the contracting templates reviewed by the ANAO to provide enhanced guidance and more clearly define contractual requirements to aid the effective implementation of the framework.

12. Defence has provided partially effective support and training to Defence contract managers in relation to the DISP. There are shortcomings in the application of DISP requirements in active contracts by its contract managers.

13. Defence has been largely effective in providing advice to industry entities about their responsibilities under the DISP. Recent activity, including the launch of a DISP website in December 2020 and the release of guidance in February 2021, has expanded the advice available to industry. While additional advice has been provided, it has not been timely given the major changes to the DISP that were announced by the Minister in April 2019. Industry has commented positively on Defence's engagement, while also identifying opportunities for improved Defence advice about the DISP.

14. Defence has not been processing DISP applications in a timely manner but has put in place surge arrangements which have resulted in an increase in the rate of processing since January 2021. Preparations for the expected increase in the number of applicants following the expansion of the program in April 2019, and the requirement for existing DISP members to reapply, were inadequate. In 2020–21, Defence commenced a project to improve overall processing timeframes and reduce the current backlog of applications. In March 2021, Defence advised the Minister for Defence Industry that it was on track to resolve the application backlog by May 2021. As at June 2021, Defence records indicate that it had received 1,267 DISP membership applications, of which 657 had been granted membership and 591 were awaiting processing.

15. As of June 2021, Defence's records indicate that of the 591 applications awaiting processing, it had not yet granted DISP membership to 237 industry entities that held an active contract with Defence. This data indicates an improvement since January 2021, when 509 industry entities that held an active contract had not been granted DISP membership. Of the 237 industry entities with an active Defence contract and awaiting DISP membership, 153 entities are in the priority 1 category (meaning the entity holds a contract with Defence to support an ongoing Defence operation).

Monitoring compliance

16. Defence has not established fit for purpose arrangements to monitor compliance with contracted DISP requirements. As at March 2021, Defence had over 16,500 active contracts with a total commitment of more than $202 billion. Defence does not know which of these contracts should, or do, require the contracted entity to have DISP membership. This situation limits the effectiveness of DISP as a security control. Further, Defence has not implemented an effective compliance and assurance framework which would allow it to assess industry entities' ongoing compliance with the DISP. Its current program provides limited to no assurance of compliance with contracted DISP requirements.

17. Defence's systems for managing DISP memberships are not considered to be fit for purpose. Internal review activity has led Defence to conclude that it has had a systemic problem with maintaining accurate records in its systems and data remediation work has been required.

18. Defence contract managers are not provided with relevant information to help them manage contractor compliance with contracted DISP requirements. There has been limited internal assurance activity to date, with four 'deep dives' of a small selection of industry completed and five 'deep dives' commenced. The results of the completed 'deep dives' have been provided to relevant Defence group

heads. Defence does not collate or analyse security incident data on DISP members that could be provided to relevant contract managers, and contract managers do not have visibility of DISP membership records.

Managing non-compliance

19. Defence has not established an appropriate framework to manage non-compliance with contracted DISP requirements. While the Defence Security Principles Framework outlines actions Defence may take against contractors for non-compliance with DISP membership requirements, Defence has not documented a framework with a clear escalation pathway for managing non-compliance.

20. In the absence of a framework for managing non-compliance with DISP requirements, it is not clear if Defence has taken appropriate action in response to identified non-compliance with its security policy. The limited assurance activity undertaken to date indicates that Defence has not made use of the full range of available actions in response to identified non-compliance with its security policy. Defence records of the nine known instances of a major security incident occurring indicate that Defence has not adopted a risk-based compliance approach or pursued any of the actions available to it under its Defence Security Principles Framework, such as contractual, criminal or financial penalties.

21. Available evidence indicates that Defence: has realised security risk; and has procured goods and services without the DISP requirements having been met.

Recommendations

Recommendation No.1

The Department of Defence review its suite of contracting templates to ensure references are to the current DISP requirements set out in the Defence Security Principles Framework.

Department of Defence response: Agreed.

Recommendation No.2

The Department of Defence ensure that contract managers receive adequate training and support in the application of Defence Security Principles Framework Control 16.1: Defence Industry Security Program, to aid understanding and compliance.

Department of Defence response: Agreed.

Recommendation No.3

The Department of Defence assure itself that its current contracts meet DISP requirements, including that:

(a) contracts include DISP membership clauses where required;

(b) contractors hold the required levels of DISP membership; and

(c) requirements for DISP membership are met by contractors on an ongoing basis.

Department of Defence response: Agreed.

Recommendation No.4

The Department of Defence, consistent with its policy on records management, ensure that supporting documentation for DISP membership applications is accurate, accessible and auditable.

Department of Defence response: Agreed.

Recommendation No.5

The Department of Defence fully implement the DISP assurance activities documented in the Defence Security Principles Framework.

Department of Defence response: Agreed.

Recommendation No.6

The Department of Defence establish a documented framework for managing non-compliance with contracted DISP requirements, with a clear escalation pathway.

Department of Defence response: Agreed.