The Auditor-General
Auditor-General Report No.4 2021–22
Performance Audit

Defence’s Contract Administration — Defence Industry Security Program

Department of Defence

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76033-677-6 (Print)
ISBN 978-1-76033-678-3 (Online)

Senior Executive Director
Corporate Management Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Or via email:
communication@anao.gov.au.

Australian National Audit Office

Canberra ACT

13 September 2021

Dear Mr President
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit in the Department of Defence. The report is titled *Defence's Contract Administration — Defence Industry Security Program*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website — http://www.anao.gov.au.

Yours sincerely

Grant Hehir
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7300
Email: ag1@anao.gov.au

Auditor-General reports and information about the ANAO are available on our website:
http://www.anao.gov.au

Audit team

Natalie Whiteley
Kim Murray
Song Khor
Clyde Muthukumaraswamy
Sally Ramsey

Contents

Audit snapshot

Auditor-General Report No.4 2021–22

Defence's Contract Administration — Defence Industry Security Program

Why did we do this audit?

- The Defence Industry Security Program (DISP) aims to support Australian businesses to understand and meet their security obligations when engaging in Department of Defence projects, contracts and tenders.
- This audit provides the Parliament with independent assurance of the effectiveness of Defence's arrangements to manage security risks when procuring goods and services.

Key facts

- The DISP is a long running program in Defence spanning several decades.
- Defence has stated that its DISP 'is essentially security vetting for Australian businesses'.
- In April 2019, the Minister for Defence Industry announced changes to the DISP which included opening the program to any Australian entity interested in working with Defence. Previously, an entity was required to already have a contract with Defence in order to apply for DISP membership.
- In 2020-21, Defence's expenditure for managing the DISP was $10 million, with 70 staff.

What did we find?

- 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 non-compliance with contracted DISP requirements.

What did we recommend?

- There are 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.

$202.4 bn

Total commitment for 16,503 active Defence contracts as at 24 March 2021.

657

Industry entities granted DISP membership between April 2019 and June 2021.

6.6 months

Average processing time for DISP membership applications from April 2019 to January 2021.

Summary and recommendations

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

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].

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 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 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.

---

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)*, available from https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/PersonnelSecurity [accessed 13 July 2021].

6 ibid., p. 24.

10. Defence has not established effective arrangements to manage identified non-compliance with contracted DISP requirements. In particular, Defence has not established an appropriate framework to manage non-compliance with contracted DISP requirements, with a clear escalation pathway. Where Defence has identified non-compliance with DISP requirements, it has not adopted a risk-based approach to compliance or pursued any of the contractual or other remediation actions available to it under the Defence Security Principles Framework.

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 510 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
Paragraph 2.7

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
Paragraph 2.22

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
Paragraph 3.21

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
Paragraph 3.38

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
Paragraph 3.47

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
Paragraph 4.8

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.*

Summary of the Department of Defence's response

22. The Department of Defence's full response can be found at Appendix 1. Defence's summary response has been included below:

> Defence acknowledges the conclusion that Defence's administration of contractual obligations relating to the Defence Industry Security Program (DISP) is partially effective. Defence agrees to implement all recommendations proposed in the report. To address these recommendations, Defence will continue a program of improvements that will enhance the effectiveness of the DISP, and also commence improvements to strengthen DISP requirements in Defence contracts.
>
> The security of Defence's people, information and assets is vital to ensuring that Defence can deliver critical capabilities. In support of the secure delivery of these capabilities, Defence is working in partnership with defence industry to improve policies, practices and outcomes to securely deliver that capability. Amongst the suite of Government initiatives and regulations intended to shape a secure and resilient defence industry sector, is the jointly developed Defence

and Australian Industry Group guide, Working Securely with Defence. This guide supports ongoing efforts to ensure defence industry is equipped with the tools and knowledge to defend against the wide range of security threats that Defence faces.

Defence has received positive feedback from industry regarding the Department's: engagement with industry; activities to expand advice and support available to industry members applying for DISP membership; and faster processing times for DISP applications since the improvement program commenced in December 2020. Defence is confident that it will continue to build on the improvements gained through the first half of 2021, with improved systems, processes and engagement for the DISP.

Furthermore, the DISP Assurance Program Framework, which was implemented across 2020 and 2021, is helping to practically improve security practices for DISP members. The Program periodically checks that DISP members are meeting Defence's security standards, and a cooperative 'uplift' component within the Program supports defence industry to improve security resilience when and where needed.

23. At Appendix 2, there is a summary of program-level improvements that were observed by the ANAO during the course of the audit.

Key messages from this audit for all Australian Government entities

24. Below is a summary of key messages, including instances of good practice, which have been identified in this audit and may be relevant for the operations of other Australian Government entities.

Performance and impact measurement

- To enable reporting on the extent to which policy objectives and outcomes have been achieved through program delivery, entities should develop performance measures when designing the delivery approach.

Program implementation

- To support the successful delivery of significant program redesign and expansion activity, entities should ensure that the activity is supported by an agreed implementation plan and appropriate levels of resourcing.
- Where program delivery involves multiple internal stakeholders, entities should ensure that their responsible business areas formalise roles, responsibilities and business processes to ensure effective end-to-end delivery and the management of shared risks.

Governance and risk management

- Where a compliance regime has been established, it is important to establish the means to analyse risk across the affected population and to focus compliance activity on areas identified as presenting a higher risk. This approach ensures that resources are appropriately allocated, commensurate with identified risk.

Audit findings

1. Background

Introduction

1.1 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.[7] 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.

1.2 Since 2016, Defence has sought to strengthen its collaboration with Australian defence industry. The *2016 Defence Industry Policy Statement* set out that:

> The Defence Industry Policy Statement provides the foundation to take the partnerships between Defence and industry to new levels of cooperation, with a focus on stronger, more strategic partnerships and closer alignment between industry investment and Defence capability needs. Initiatives in the Defence Industry Policy Statement will see the development of a technologically advanced, innovation-driven and sustainable Australian defence industrial base, which is well placed to assist Defence in protecting Australia's national interests.[8]

1.3 Under the Australian Government's Protective Security Policy Framework (the PSPF)[9], Defence is responsible for protecting its people, information and assets including through its contractual arrangements. The PSPF states that:

> Non-government organisations that access security classified information may be required to enter into a deed or agreement to apply relevant parts of the PSPF for that information.[10]

7 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.

8 Department of Defence, *2016 Defence White Paper*, At a Glance, available from https://www.defence.gov.au/Whitepaper/AtAGlance/Defence-Industry.asp [accessed 12 May 2021].

9 The PSPF applies to non-corporate Commonwealth entities subject to the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) to the extent consistent with legislation. The PSPF sets out government protective security policy in terms of: security governance; information security; personnel security; and physical security. Source: Attorney-General's Department, *Protective Security Policy Framework*, available from https://www.protectivesecurity.gov.au/ [accessed 8 January 2021].

10 Attorney-General's Department, *Application of the Protective Security Policy Framework*, available from https://www.protectivesecurity.gov.au/about/Pages/application-protective-security-policy-framework.aspx [accessed 12 May 2021].

1.4 To implement the requirements of the PSPF and the Australian Government Information Security Manual[11], Defence established the Defence Security Principles Framework (DSPF) in 2018.[12] The DSPF is both a key enterprise-level control for managing security risk and the primary security policy for Defence personnel, contractors, consultants and outsourced service providers. Under the DSPF, Defence Security Principle 16 – Defence Industry Security Program (DISP), states that:

> DISP enhances Defence's ability to manage risk in the evolving security environment and provides confidence and assurance to Defence and other government entities (either Australian or foreign) when procuring goods and services from industry members.[13]

1.5 Defence Security Principle 16 sets out the following expected outcomes:

> Accountabilities and responsibilities for security risk management when procuring goods and services are understood and practised.
>
> Security risks are effectively and efficiently managed between Defence and industry.
>
> DISP:
>
> a. supports Defence's agility in achieving value for money in procurement;
>
> b. provides effective and efficient mechanisms for certifying and accrediting industry's security practices;
>
> c. enables increased access to security tools and information to strengthen industry security practices; and
>
> d. delivers confidence and assurance when partnering with industry, underpinned by proportional (risk based) oversight and compliance activities.[14] [15]

1.6 The DISP aims to support Australian businesses to understand and meet their security obligations when engaging in Defence projects, contracts and tenders. The Defence website states that the DISP is 'essentially security vetting for Australian businesses'.[16]

---

11 The purpose of the Australian Government Information Security Manual (ISM) is to outline a cybersecurity framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats. Source: Australian Cyber Security Centre, *Australian Government Information Security Manual*, January 2021, available from https://www.cyber.gov.au/sites/default/files/2021-01/Australian%20Government%20Information%20Security%20Manual%20%28January%202021%29.pdf [accessed 8 January 2021].

12 The DSPF replaced the Defence Security Manual (DSM) on 2 July 2018.

13 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 12 May 2021].

14 ibid.

15 The DISP is one of four principles and controls that address security supply chain risk. The other three are: Principle 11 and Control 11.1 – Security for Projects; Principle 12 – Security for Capability Planning; and Principle 82 – Procurement. Source: Department of Defence, *Defence Security Principles Framework*, 31 July 2020, available from https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf [accessed 7 July 2021].

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

The Defence Industry Security Program

1.7 The DISP is a long running program in Defence spanning several decades. Since at least 1978, Defence has had a documented security policy framework that incorporates the DISP. Since at least 2000:

- The principal purpose of the program has remained relatively unchanged, with a focus on: addressing the threat to Defence industry companies and others in the private sector who require access to national security classified material; and defining the mandatory minimum standards, policies and procedures to ensure the protection of classified material entrusted to Australian industry.
- The Defence Security and Vetting Service and its predecessors (Defence Security Branch and the Defence Security Authority) manage the DISP on behalf of Defence. The head of that organisational element within Defence has remained responsible for the design and administration of the DISP, with Defence personnel (as managers of contracts) responsible for implementing the requirements of the DISP within Defence's contracted activities.

1.8 More recently, the criteria for industry entities to access the DISP have been adjusted. 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, different levels of DISP membership based on security classifications were introduced. The Minister described these as 'major reforms' to the DISP and stated that:

> The reforms will maximise the benefits to Australian businesses from the unprecedented investment in defence industry by the Australian Government while providing better security outcomes for Australia.
>
> … the reforms would allow DISP members to easily access security information, guidance and services and enable them to become 'Defence-ready' by establishing the necessary security practices for tendering opportunities involving classified information and assets.[17]

1.9 In July 2020, Defence completed a review of the operation of the DISP which identified a number of issues including:

- a significant, and growing, backlog of applications with no ability to scale-up to manage the expected increase in applications and reaccreditation of existing participants;
- insufficient resourcing;
- poor DISP membership registry technology support, with low data quality to manage participant details and status;
- interdependencies in application processing and management contributing to increased processing times;
- no clear processes for managing and escalating participant non-compliance with DISP membership requirements; and

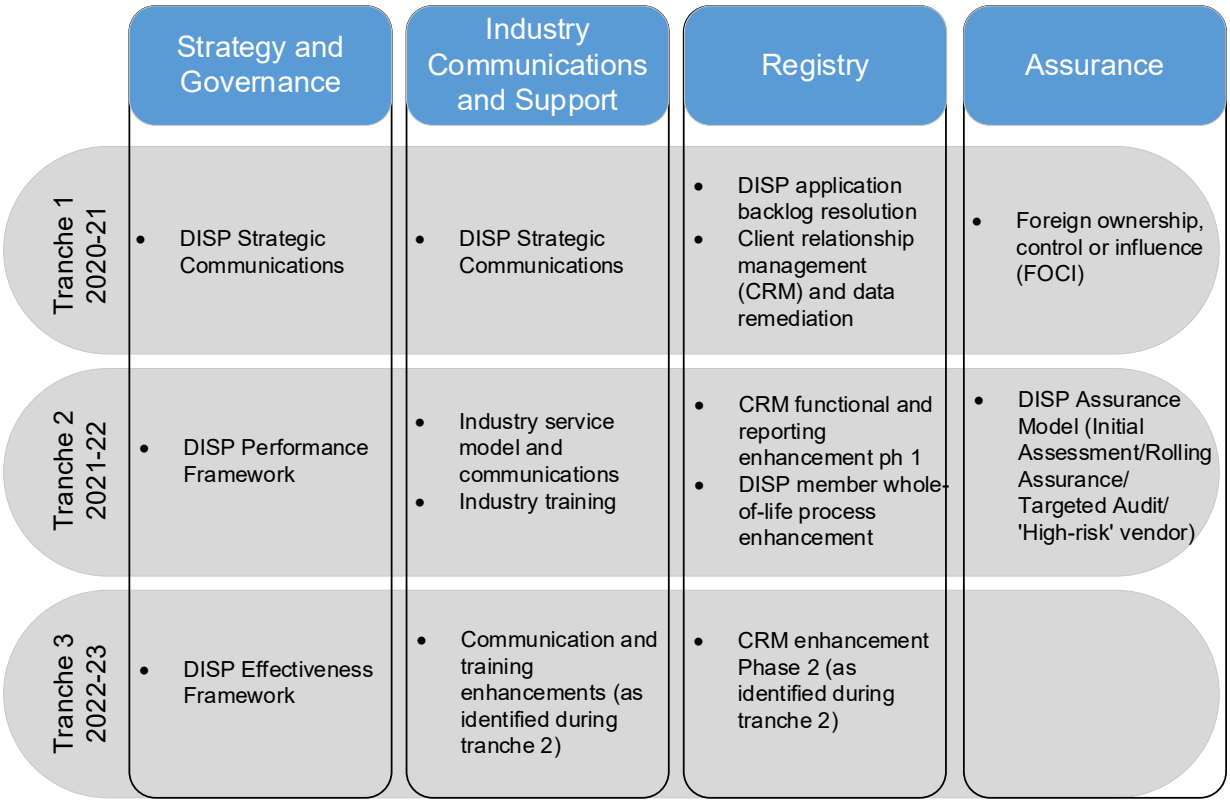
17 Minister for Defence Industry, *Major reform to Defence Industry Security Program*, 5 April 2019, available from https://www.minister.defence.gov.au/minister/linda-reynolds/media-releases/major-reform-defence-industry-security-program-1 [accessed 14 May 2021].

- an over emphasis on application processing with insufficient focus on assurance activities to ensure DISP members are continuing to meet security requirements.

1.10 The DISP Improvement Program is intended to address a number of shortcomings Defence identified in its review of the operation of the DISP.

1.11 In late 2020, Defence commenced implementation of the DISP Improvement Program Plan (see Figure 1.1 below) which is comprised of four streams of work that are to be delivered in three tranches in 2020–21, 2021–22 and 2022–23.

Figure 1.1: DISP Improvement Program projects by tranche



Source: Defence documents.

1.12 A timeline of events in the DISP that are relevant to this audit, is set out in Appendix 3.

Implementation of DISP in Defence's contractual arrangements

1.13 The 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[18]; storing or transporting

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

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.[19]

1.14 An industry entity may be exempt from DISP membership where the entity has an accreditation recognised under a Security of Information Agreement or Arrangement, or personnel are handling official information within Defence facilities and using Defence assets.[20]

1.15 The application process for DISP membership is outlined at Appendix 4. The support provided to industry to obtain DISP membership and the timeliness of Defence's processing of DISP applications is discussed in Chapter 2.

1.16 The security requirements that the industry entity is expected to meet as a DISP member increase with the sensitivity of the material being accessed. Figure 1.2 illustrates the relationship between the four DISP membership levels (entry level to level 3), the four security elements (governance, personnel security, physical security, and ICT and cybersecurity) and security classifications for information and assets.

Figure 1.2: Mapping DISP membership levels to security elements and security classifications

	Governance	Personnel Security	Physical Security	ICT and Cybersecurity
Entry Level	OFFICIAL/ OFFICIAL: Sensitive	OFFICIAL/ OFFICIAL: Sensitive	OFFICIAL/ OFFICIAL: Sensitive	OFFICIAL/ OFFICIAL: Sensitive
Level 1	PROTECTED	PROTECTED	PROTECTED	PROTECTED
Level 2	SECRET	SECRET	SECRET	SECRET
Level 3	TOP SECRET	TOP SECRET	TOP SECRET	TOP SECRET

Source: Defence documentation.

1.17 The details schedule in Defence's template contract is expected to capture if DISP membership is required, and if so, the level of membership required for each security element. For contracts requiring DISP membership, the conditions of contract should include a specific clause on obtaining and maintaining DISP membership (see Box 1 below). In addition to a clause on DISP membership, Defence contracts may include other security clauses, including clauses on accessing security classified information or accessing Commonwealth premises. Box 1 provides an example of a DISP clause in a contracting template.

19 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.

20 Defence advised the ANAO in December 2020 that it does not have a record of industry entity exemptions to DISP membership, and that only Australian entities are eligible to join the DISP. Defence further advised the ANAO in June 2021 that DISP membership may not be required if contracted personnel have an appropriate personnel security clearance, handle classified information within Defence facilities and use Defence assets /ICT networks. In this instance, governance is managed by a Defence Security Officer.

Box 1: Example of a DISP clause in a Defence contracting template

The security classification of the information and assets accessible to the Contractor and work to be performed under the Contract will be up to and including the level specified in the Details Schedule. The Contractor shall:

a. obtain and maintain all elements of DISP membership at the levels specified in the Details Schedule (or an equivalent international agreement or arrangement) in accordance with Principle 16 of the DSPF.

Source: Defence documentation.

1.18 An example of how the DISP applied to the delivery of security vetting services by contracted service providers was provided by Defence in the context of the Joint Committee of Public Accounts and Audit's inquiry into Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security*. Defence advised the committee that in the case of companies that are contracted to provide positive vetting services, there is:

> Due diligence through our contract requirements and through the requirements of them to report as DISP members. So the contract requirements are part of the industry security program, so they have reporting obligations to report against those requirements. And we have an audit and assurance program required under that industry program membership against your physical security, your information security, the delivery of your training and the requirements to meet those industry program mandatory requirements.[21]

1.19 Defence's arrangements for monitoring compliance and managing non-compliance with DISP requirements are discussed in Chapters 3 and 4. Issues in relation to Defence's management of compliance with DISP requirements and the management of industry security risk in Defence have been identified previously, through a review in 2017. The review included six recommendations that are relevant to this performance audit. On 20 June 2017, the Australian Government agreed to all of the recommendations from the review. Appendix 5 sets out the six recommendations and the status of their implementation.

DISP administration and budget

1.20 Within Defence, the Defence Security and Vetting Service (DS&VS) is responsible for administering the DISP, through its Defence Industry Security Office (DISO).

1.21 The DSPF sets out the roles and responsibilities of Defence (both DS&VS and Defence contract managers) and industry entities in the context of the DISP. These are outlined in Table 1.1 below.

21 Official Committee Hansard, Joint Committee of Public Accounts and Audit, inquiry into Personnel security, domestic passenger screening—Auditor-General's reports 38 and 43 (2017-18), 12 February 2019 available from https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commjnt/af2f69ce-f737-4fcd-9c98-3e933e4efe37/&sid=0000 [accessed 2 June 2021].

Table 1.1: DISP roles and responsibilities — Defence and industry entities

Defence Security and Vetting Service (DS&VS)	• Defence Industry Security Office (DISO) within DS&VS administers DISP application and assessment process, and undertakes DISP assurance activities • First Assistant Secretary (FAS) DS&VS is responsible for granting DISP membership • Assistant Secretary Security Policy and Services: – control owner for DISP – accountable for effective implementation reports annually to Defence Security Committee[a] on effectiveness of DISP controls
Defence contract managers[b]	• assess and manage project security risk • determine whether an industry entity should hold DISP membership and at what level • ensure that obtaining and maintaining the appropriate level of DISP membership is a condition of contract • ensure that industry entity holds the appropriate level of DISP membership before the contract is signed and the contracted activities commence
Industry entity	• provide all relevant information to Defence to assess their suitability and eligibility for DISP • ensure ongoing suitability with DISP requirements including meeting all security requirements specified by Defence and any Australian Government entity in a contract or Security of Information Agreement or Arrangement

Note a: The Defence Security Committee provides primary oversight of the DSPF. Control Owners are required to provide an annual report to the Defence Security Committee on each DSPF Principle and expected outcome for which they have responsibility.

Note b: In the context of managing DISP requirements, Defence defines contract managers as: 'Defence personnel responsible for managing Defence contracts; this could include but is not limited to, Program Managers, Project Managers, Senior Project Officers, Project Officers or any other role with contract manager responsibilities'.

Source: ANAO analysis of Defence documentation, and Defence advice.

1.22 Table 1.2 below provides a summary of DS&VS's actual expenditure and staffing levels attributed to managing the DISP during 2019–20 and 2020–21. Defence advised the ANAO in June 2021 that the DISP operating budget for 2021-22 is $6 million and additional funding is being sought through the Defence budget process.

Table 1.2: Defence Security and Vetting Service – actual expenditure and staffing levels for managing the DISP 2019–20 and 2020–21

2019–20 expenditure and staffing levels	2020–21 expenditure and staffing levels
$1.206 million	$10 million
• 6 APS staff • 12 contractors	• 12 APS staff • 58 contractors

Source: Defence documentation.

1.23 On its external website for the DISP, Defence advises that:

> There is no direct cost associated with DISP membership (i.e. no membership fee), however, there will be costs associated with implementing and maintaining security measures to meet both initial and ongoing DISP membership requirements. These might include, for example, facility certification and accreditation, personnel security clearances, physical security measures.[22]

Rationale

1.24 Defence has stated that its Defence Industry Security Program (DISP) 'is essentially security vetting for Australian businesses'.[23] 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.[24] 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'.[25] This audit provides the Parliament with 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 approach

1.25 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).

1.26 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?

22 Department of Defence, Defence Industry Security Program, How to Apply webpage: https://www1.defence.gov.au/security/industry/how-apply#Cost [accessed 15 April 2021]. Defence advised the ANAO in June 2021 that while cost recovery methods have been considered the DISP remains free at this stage.

23 Department of Defence, Defence Industry Security Program webpage: https://www1.defence.gov.au/security/industry [accessed 31 May 2021].

24 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)*, available from: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/PersonnelSecurity [accessed 13 July 2021].

25 ibid., p. 24.

1.27 The audit focussed primarily on Defence's:

- administration of DISP as it relates to contractual obligations, including Defence's communication of DISP requirements to industry and Defence contract managers, and relevant training and support; and
- monitoring and assurance activities for ensuring DISP members' compliance with contracted DISP requirements, including any actions taken to address non-compliance with contracted obligations.

1.28 The audit did not:

- assess the decisions made by Defence officials regarding the level of DISP membership required during tendering and contract establishment processes;
- assess the effectiveness of Defence's DISP membership assessment process (that is, the process supporting the decision to grant membership), or re-assess decisions to issue DISP membership; or
- test specific contracts to confirm that contracted DISP membership requirements had been addressed, due to limitations in Defence systems and processes discussed further below.

Audit methodology

1.29 The audit involved:

- a review of documentation held by the department, including policies, processes and procedures;
- discussions with relevant departmental staff and industry stakeholders; and
- analysis of Defence data.

1.30 The ANAO planned to review a statistically valid sample of Defence contracts as part of this performance audit, to assess whether contracts that require DISP membership include an appropriate DISP clause, that the contractors engaged for those contracts have DISP membership, and that the contractor's DISP membership for those contracts is at the appropriate level. For this purpose, the ANAO sought from Defence a list of current contracts that included a clause requiring the contracted industry entity to hold a DISP membership. However, Defence was unable to provide a complete and accurate list of contracts that included a DISP requirement, to enable the selection of a statistically valid sample for ANAO review.

1.31 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately $400,712.

1.32 The team members for this audit were Natalie Whiteley, Kim Murray, Song Khor, Clyde Muthukumaraswamy and Sally Ramsey.

2. Administering contracted DISP requirements

Areas examined
This chapter examines whether Defence has established fit-for-purpose arrangements for administering contracted DISP requirements.

Conclusion
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.

Area for improvement
The ANAO made two recommendations aimed at ensuring that: contracting templates are consistent with DISP requirements as set out in the Defence Security Principles Framework (DSPF); and that Defence contract managers receive adequate support and training on DSPF Control 16.1 — Defence Industry Security Program, to aid understanding and compliance.

2.1 This chapter examines whether Defence has established fit-for-purpose arrangements for administering contracted DISP requirements. Fit-for-purpose arrangements underpin good program and risk management by clarifying roles and responsibilities and supporting the effective implementation of key activities. The ANAO examined whether Defence has:

- clearly defined DISP requirements to guide Defence officials, particularly its contract managers and Defence Industry Security Office (DISO) personnel, through their responsibilities regarding the DISP;
- supported and trained contract managers to understand their responsibilities for implementing the DISP;
- advised industry entities about their responsibilities under the DISP; and
- established arrangements to process DISP applications in a timely manner to support contract managers and industry to address DISP requirements effectively.

Does Defence have a framework that clearly defines DISP requirements?

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.

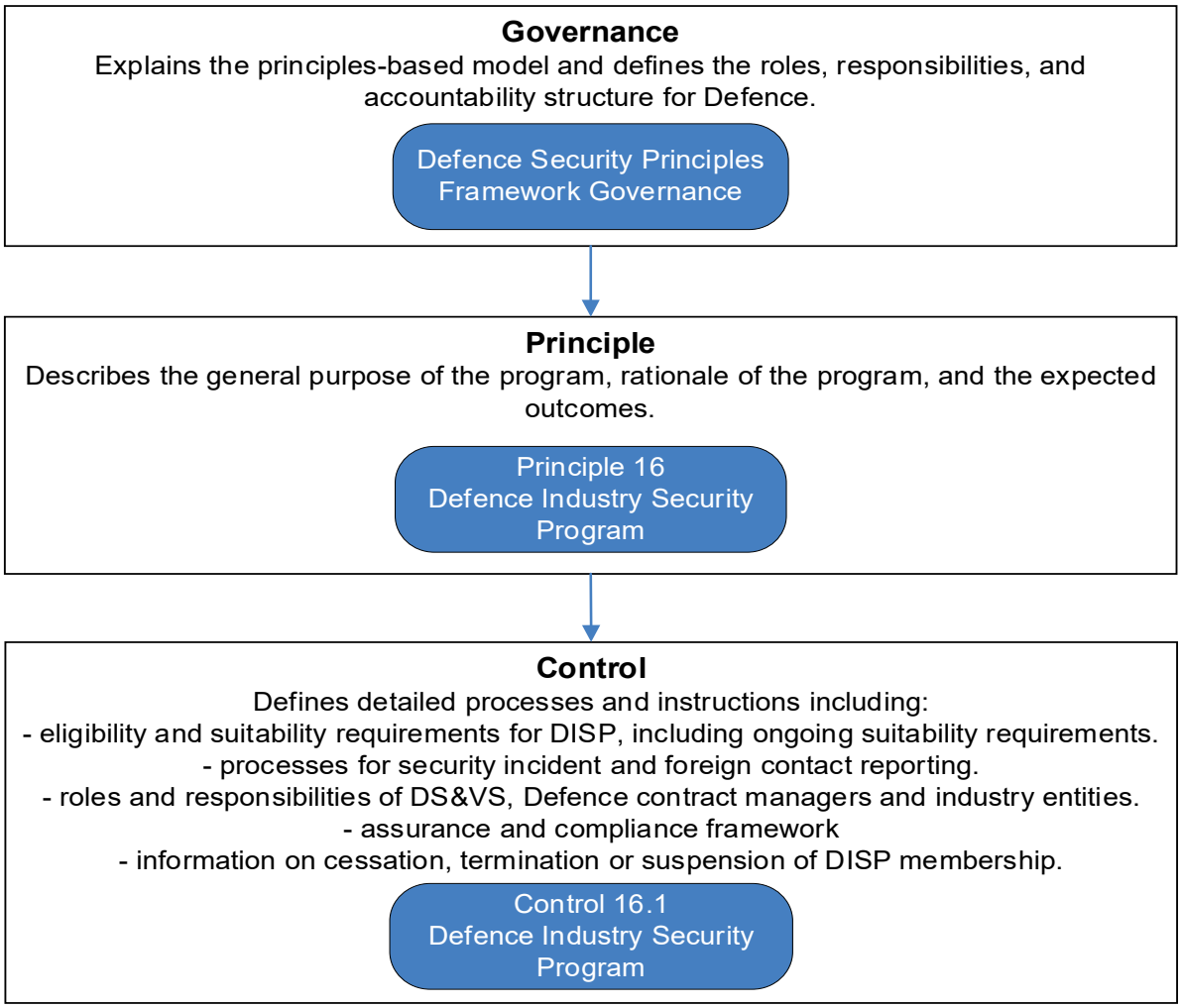
2.2 For DISP to be implemented effectively across Defence, clear guidance on the policy requirements and their implementation is necessary. The ANAO reviewed whether:

- DISP requirements are clearly defined in Defence's security policy documents; and
- DISP requirements are clearly defined in Defence's contracting templates.

Policy documents

2.3 The Defence Security Principles Framework (DSPF) includes two documents specifically relating to the DISP — a principles document (Principle 16) and a controls document (Control 16.1) (as shown in Figure 2.1 below). Control 16.1 sets out the requirements of the DISP.

Figure 2.1: How the DISP is defined within the Defence Security Principles Framework



Source: ANAO analysis of Defence documents.

Contracting templates

2.4 In its review of the DISP in July 2020, Defence states that:

> Defence Industry's obligation to manage security risk in accordance with DSPF requirements is articulated within contractual arrangements between Defence and Defence Industry. As a result, contract managers in Defence have primary responsibility for ensuring Defence Industry complies with security risk management arrangements outlined in contractual arrangements.
>
> When Defence assesses the security risk of an activity (e.g. project delivery, capability sustainment) to be higher than can be readily managed under standard contractual arrangements,

the contract manager may require that the Defence Industry member is a participant in the Defence Industry Security Program (DISP).[26]

2.5 As at February 2021, Defence had three main contracting templates for contracts valued at $200,000 or greater.[27] [28] Defence advised the ANAO that these are the:

- Australian Standard for Defence Contracting (ASDEFCON), administered within Defence's Capability Acquisition and Sustainment Group[29];
- Defence Facilities Suite of Contracts, administered within Defence's Estate and Infrastructure Group; and
- Information Communications Technology Provider Arrangement, administered within Defence's Chief Information Officer Group.[30]

2.6 The ANAO reviewed these three main contracting templates to assess whether DISP requirements had been clearly defined. The contracting templates included various mandatory requirements and guidance for contract managers on the use of DISP clauses in contracts.[31] There were opportunities for the templates to provide enhanced guidance and more clearly define contractual requirements, by:

- including a mandatory clause specifying if DISP membership is, or is not, required;
- requiring the contract drafter to specify the level of DISP membership the industry entity must hold for each of the four security elements of the DISP; and
- referencing current security policy.

---

26 Defence advised the ANAO that 'the requirement to participate in the DISP is not the sole security control required to manage risk which is assessed as 'higher than can be readily managed under standard contractual arrangements' – rather, DISP membership is one tool which complements mitigation efforts and which provides a baseline understanding about the entity's security posture and performance maturity.'

27 Non-corporate Commonwealth entities must use the Commonwealth Contracting Suite (CCS) when purchasing goods or services valued under $200,000 (GST inclusive) where a formal contract is required, except where a specific exemption applies. The CCS, administered by the Department of Finance, does not reference Defence specific policy such as the DISP. The CCS was not examined in this performance audit. Defence advised the ANAO in June 2021 that: 'The CCS does not contain DISP clauses and is therefore is not [sic] suitable for contracts with security requirements which necessitate the contractor to hold a DISP membership'. Defence further advised the ANAO in August 2021 that: 'in instances where the CCS is not suitable, such as where DISP membership or security requirements are needed, the ASDEFCON suite of tendering and contracting templates should be used'.

28 In June 2021, after the conclusion of ANAO fieldwork, Defence provided the ANAO with 25 additional templates, part of the Defence Science Partnering Deed and associated templates, and the Strategic, Research and Development Alliances. These additional templates have not been assessed by the ANAO, on the basis of advice from Defence (CASG) in February 2021 that the three templates listed in paragraph 2.5 were the three main suites of templates used across Defence.

29 In December 2020, the Minister for Defence Industry announced a review of the ASDEFCON templates, which is expected to be finalised by mid-2021.The terms of reference for the review are available from: https://www1.defence.gov.au/sites/default/files/2020-12/ASDEFCON%20%26%20Defence%20Procurement%20Review%20Terms%20of%20Reference_0.pdf [Accessed 8 January 2021].

30 In June 2021, Defence advised the ANAO that this suite of templates has been withdrawn from use.

31 Defence informed the ANAO in June 2021 that: 'The different contract templates across Defence's delivery groups reflect the differing nature of the goods and services being delivered'.

Recommendation no. 1

2.7 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.*

Has Defence provided effective support and training to Defence contract managers relating to DISP requirements?

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.

2.8 DSFP Control 16.1 — Defence Industry Security Program, states that:

> Contract Managers must notify DS&VS [the Defence Security and Vetting Service] where DISP membership is a contract requirement. Contract managers must provide DS&VS with the following information:
>
> a. the Defence representative contact details;
>
> b. the Entity Defence is engaging with;
>
> c. details of the contract/panel/partnership;
>
> d. the security requirements of the contract/partnership including DISP membership levels. For example governance level 'x', personnel security level 'x', physical security level 'x', information/cyber security level 'x'.

2.9 As at 30 June 2019 and 30 June 2020, Defence's Assistant Secretary, Security Policy and Services (the control owner), assessed the implementation of DSPF Control 16.1 Defence Industry Security Program, as 'developing'. In this context, 'developing' means: 'the DSPF Control is implemented, broadly managed and understood across Defence. Defence is largely meeting the DSPF Expected Outcome'. In July 2021 the ANAO sought the control owner's 30 June 2021 assessment report. Defence advised the ANAO in August 2021 that the assessment report was not yet finalised.

2.10 The ANAO examined the guidance, support and training provided to contract managers to support their implementation, management and understanding of the control.

Guidance and support available for contract managers

2.11 Guidance for Defence's contract managers includes Defence's mandatory procurement policy (the Defence Procurement Policy Manual), and a range of handbooks, guides and factsheets.[32] Notwithstanding the available guidance, Defence's July 2020 review of the DISP found that the DISP was poorly integrated and understood within Defence:

32 In October 2019, Defence estimated that it had around 900 policies relating to procurement.

There are many touch points and overlaps between DISP and other areas such as procurement and contract management, security risk assessment and management, program and project management, and training. Understanding of what DISP is (and isn't) is poorly understood and there is no clear understanding across the organisation of how supply chain security risk is supported and assured.

2.12 The ANAO identified gaps in Defence's extant contract management tools and guidance that was available during audit fieldwork to inform contract managers about the DISP. In particular:

- Defence had not included references to the DISP in its operational guidance to support Defence contract managers (specifically, on the Defence intranet page relating to 'managing Defence contracts').
- There was no specific operational guidance that advised contract managers on procedures for contract executions and/or service delivery under contracts where membership is required but not in place, or is not at the appropriate level of membership.
- Defence had not developed a single source of authoritative operational guidance to assist contract managers to accurately and consistently incorporate DISP requirements into contracts and to monitor industry compliance with contractual obligations.

2.13 The ASDEFCON templates are not the only templates used by contract managers to establish contracts on Defence's behalf. DISP requirements need to be considered, as necessary, regardless of the template employed. Further, there may be a need to consider DISP requirements after a contract is entered into. A 2019 review by Defence of its DISP membership records identified instances of contractors without valid DISP memberships handling classified information as part of an extant Defence contract (see paragraphs 4.10–4.16). More recently, the ANAO's review of DISP membership data as at January 2021 found that of 873 applicants who had not yet been granted DISP membership, 419 had existing contracts with Defence worth $22 billion (see paragraph 3.16).

2.14 Defence has identified that there is a need for clearer guidance to help Defence contract managers navigate the DISP throughout the procurement lifecycle. In November 2020, Defence advised the ANAO that it has established a DISP helpdesk and 'DISP.info' email address, and is in the process of:

- developing a 'Defence Industry Security Program Decision Tree' with the aim of helping Defence project and contract managers navigate the DISP within the Defence procurement lifecycle'.[33] In June 2021, Defence advised the ANAO that the decision tree was published on the DISP intranet page on 4 May 2021. Defence further advised that while the decision tree has not been actively promoted across Defence, it 'will be promoted as a feature product for Contract Managers to use, when the DISP intranet page is launched later this year';
- redeveloping the DISP intranet page. In December 2019, the Defence Security and Vetting Service advised the Defence Security Committee that the redeveloped intranet page would: 'better support Defence contract and project managers on the DISP, how it can be used as a risk mitigating tool and increase visibility on existing Defence contracts with industry' and that it was due to be launched in early 2020. Defence advised the ANAO in

33 In the context of managing DISP requirements, the Defence procurement lifecycle comprises: initiation; evaluating tenders; awarding a contract; managing a contract; and closing a contract.

January 2021 that the revised DISP intranet site would be launched in early 2021. Defence advised the ANAO in June 2021 that the DISP intranet page will be launched later in 2021; and

- developing an internal stakeholder engagement plan and communications for DISP, with implementation expected in early 2021. Defence developed a communications action plan that was endorsed on 26 March 2021.

Training available for contract managers on DISP requirements

2.15 Defence informed the ANAO in October 2020 that there is a DISP awareness and contract manager training course. The training consists of a brief presentation that provides a high level overview of the DISP program, with limited information on the roles and responsibilities for contract and project managers in relation to DISP requirements.

2.16 Defence informed the ANAO in February 2021 that as of 24 November 2020, 205 completions were recorded since release, which includes 84 completions between May and November 2020. Defence further advised that a formal assessment measuring the effectiveness of this course has not been undertaken, and that:

> The course remains useful in the absence of an adequate intranet presence of DISP information for contract/project managers. Once this intranet presence is created, the course in its current format will likely be redundant.

2.17 The 205 completions represent a small percentage of the at least 1500 contract managers across Defence, noting that Defence estimated that as of May 2021, there were approximately 858 contract managers in CASG alone. Further, Defence informed the ANAO in June 2021 that:

> Defence is not able to give an exact figure of contract managers across the enterprise, noting widespread and distributed delegation of contract management. For example:
>
> - Capital Facilities and Infrastructure, as part of Estate & Infrastructure Group, has 69 contract managers;
> - Defence Science and Technology Group has 576 lead researchers who are the contract managers for 1331 current agreements;
> - Joint Logistics Command has 35 contract managers.

2.18 In February 2021, the First Assistant Secretary of the Defence Security and Vetting Service advised the Associate Secretary that outreach and education for the DISP was 'missing all or most capability', including having: 'dedicated stakeholder communications, information and communication for Defence about DISP'.

2.19 Defence's July 2020 DISP Improvement Plan[34] had noted the limitations in Defence's support and training offered to contract managers, and identified a number of changes Defence would need to implement to address these shortcomings, including:

34 In May 2020, Defence engaged Synergy Group Australia to review the operation of the DISP and develop a DISP Improvement Plan to consolidate existing security reform projects into an integrated, prioritised improvement program.

- developing supply chain security risk management training for Defence contract managers and project managers to ensure security risk is being identified and managed appropriately;
- undertaking an internal scan of existing training to support contract and project managers to support security risk management knowledge and understanding; and
- developing tailored training and education programs for Defence contract and project managers to improve supply chain security assessment.

2.20 In February 2021, the Defence Security and Vetting Service advised the ANAO that it had completed consultation with stakeholders from across Defence to identify current information gaps and communication tools and products to address these issues. Defence further advised that the results of the consultation will inform the development of a communications action plan, to be implemented in the first quarter of 2021. As discussed in paragraph 2.14, the plan was approved in March 2021.

2.21 The limited training available on DISP reduces the level of assurance available to Defence management regarding contract managers' ability to comply with security policy when applying DISP clauses in the contracts they administer. Further, without knowing how many contract managers Defence has operating, it will be difficult to obtain assurance that adequate support and training has been provided to address the risk of non-compliance with security policy.

Recommendation no. 2

2.22 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.*

Has Defence effectively advised industry entities of their responsibilities under the DISP?

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.

2.23 In November 2020 Defence advised the ANAO that communication material had been developed, and support put in place, for industry and Defence. These activities include:

- the development of a communication strategy;
- a range of products to communicate the changing DISP requirements to industry including the development of the DISP external website, an online training course, and a national roadshow of events to publicise the changes;

- notification in April 2020, to all extant members[35] of the program, changes and requirements to transition to the new program before April 2021; and
- a helpdesk to provide support to stakeholders with questions on the program and its requirements.

Defence's communication strategy for the DISP

2.24 Defence produced a communication strategy for DISP in March 2019. The purpose of the strategy was to: 'define a tactical approach for effectively communicating the new DISP reform, including awareness, by providing information to encourage participation and to acquire a DISP membership'.

2.25 The strategy identifies its primary measurable objective as 'increase in membership', with a secondary goal of 'improved sentiment/attitudes towards, and clearer communications [of the DISP]'. The focus of the strategy is on communicating the benefits of DISP to small and medium enterprises in order to drive membership acquisition and develop capability for Defence industry. The document does not identify the program as a key security risk management strategy for Defence as identified in the program rationale in the DSPF, or include strategies for communicating information on the Defence contract manager's role in managing DISP obligations in relevant contracts.

Launch of updated external DISP website in December 2020

2.26 Defence launched an external DISP website on 11 December 2020. The updated website includes links to relevant policy documents on the DISP and government security clearances; clear and concise information on how to apply for DISP membership; factsheets, guides and tools; and information on the DISP assurance framework.

Release of DISP guide for industry in February 2021

2.27 In December 2019, Defence told the Defence Security Committee that it was developing a guide for industry on DISP membership that would be released in February 2020. The guide, *Working Securely with Defence: A guide to the Defence Industry Security Program*, was released on 22 February 2021. Defence informed the ANAO in June 2021 that:

> The *Working Securely with Defence: A guide to the Defence Industry Security Program* guide was distributed to selected industry small-medium sized enterprises (SMEs) in June 2020 following discussions in previous months to run a pilot of the product (as it then stood) and obtain feedback from real-life users.
>
> Based on the feedback from SMEs who participated in the pilot, the content of the guide was amended, the formatting and design was finalised, and appropriate stakeholders were again consulted (e.g. the Defence Ministerial and Executive Coordination and Communication Division).
>
> Several months of work was then conducted to implement all the suggested changes, and improve the overall integrity of the guide.

35 DISP members that were granted membership prior to April 2019.

2.28 The guide was developed by Defence, the Australian Industry Group Defence Council[36], the Australian Signals Directorate, the Australian Security Intelligence Organisation and the Australian Cyber Security Centre. The guide brings together information on various aspects of Defence security policy, including the DISP, for industry entities. It includes:

- background on the Defence security environment;
- an overview of DISP membership including eligibility requirements, industry benefits, application processing timeframes, and expected costs;
- advice for industry on how to apply for DISP membership including building evidence to support an application;
- an overview of each security element of DISP membership (governance, personnel, physical, ICT); and
- an outline of ongoing DISP membership obligations including participation in audit and assurance activities, working in the Defence industry supply chain, and how to report security incidents.

DISP members granted membership prior to April 2019

2.29 As part of the 'major reforms' to the DISP announced by the Minister for Defence Industry in April 2019, existing members were required to reapply for DISP membership. Defence informed the ANAO in March 2021 that 312 DISP members had been granted DISP membership prior to April 2019. Of these 312 members, as at 23 February 2021, 266 had submitted a new DISP membership application as required. In respect to the remaining 46 companies, Defence advised the ANAO in February 2021 that:

> DISO is undertaking another round of direct engagement with each of the remaining 46 companies to encourage their application into the reformed DISP. DISO will contact each listed contract/project manager to advise them of the entity's non-compliance with Defence security policy for any active pre-reform entities who fail to re-apply to the program before the deadline. Pre-reform membership will no longer be recognised after 9 April 2021, unless the entity is undergoing current DISP processing … DISO will work with each contract/project manager to make arrangements to reach compliance and/or mitigate any outstanding security risks with the project and industry partner.

2.30 Defence further advised the ANAO in June 2021 that:

> Multiple steps were taken to contact all extant members from the 'old DISP program' over the two year transition period, with a reminder to re-apply to the then 'new DISP'. A dedicated team was assigned to contact all DISP members listed in DISMS[37], and to provide any support to entities that re-applied as a direct result of the outreach activities.

2.31 On its external website, Defence advises industry that 'existing DISP members are unable to enter into a new contract, or amend an existing contract, until they successfully transition to the

36 The Australian Industry Group Defence Council is a national representative body for the Australian defence industry: https://www.aigroup.com.au/sectors-and-advocacy/Defence/ [accessed 29 January 2021].

37 Defence Industry Security Management System (DISMS) contains the membership records for DISP applications received by Defence prior to 1 April 2019. This system, and Defence's efforts to remediate the data held in it, is discussed in Chapter 3 of this report.

new program.'[38] This advice was not included in Defence emails sent in April 2020 to DISP members that were granted membership prior to April 2019, encouraging them to reapply for DISP membership.

Industry feedback on Defence communications

2.32 The ANAO reviewed Defence's records of industry engagement on the DISP during 2020, and sought feedback from industry stakeholders[39] on the communication and support offered through the DISP.

2.33 Industry stakeholders expressed broad satisfaction with the engagement from Defence since the program was opened to all of industry in April 2019. They also identified some areas for improvement, including a lack of clear guidance on the DISP and Defence security requirements for smaller and medium sized enterprises with little to no experience of working with Defence, and long processing times for DISP membership applications. Application processing times are discussed below.

Does Defence process DISP applications in a timely manner?

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 and 591 were awaiting processing.

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 510 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).

2.34 Timely processing of DISP membership applications assists contract managers to establish valid contracts that support Defence's purposes and the efficient and effective management of

38 Department of Defence, Defence Industry Security Program, DISP FAQs webpage: https://www1.defence.gov.au/security/industry/faqs [accessed 28 April 2021].

39 The ANAO sought feedback from the Australian Industry Group; the Australian Industry and Defence Network; Australian Defence Alliance Victoria; and Victorian Defence Alliances.

security risk. Delays in DISP membership processing could affect a company's ability to be 'Defence ready' and successfully bid for and win Defence contracts.[40]

2.35 The ANAO examined the timeliness of Defence's processing of DISP applications by reviewing the number of applications received, the timeframes for processing applications, and the prioritisation of applications for processing.

Number of applications received

2.36 In February 2021 the First Assistant Secretary, Defence Security and Vetting Service, advised the Associate Secretary of Defence that DISO had received 1100 membership applications since the program was opened to any industry entity in April 2019.[41] Of these 1100 membership applications, DISO had granted 230 DISP memberships up to that time.

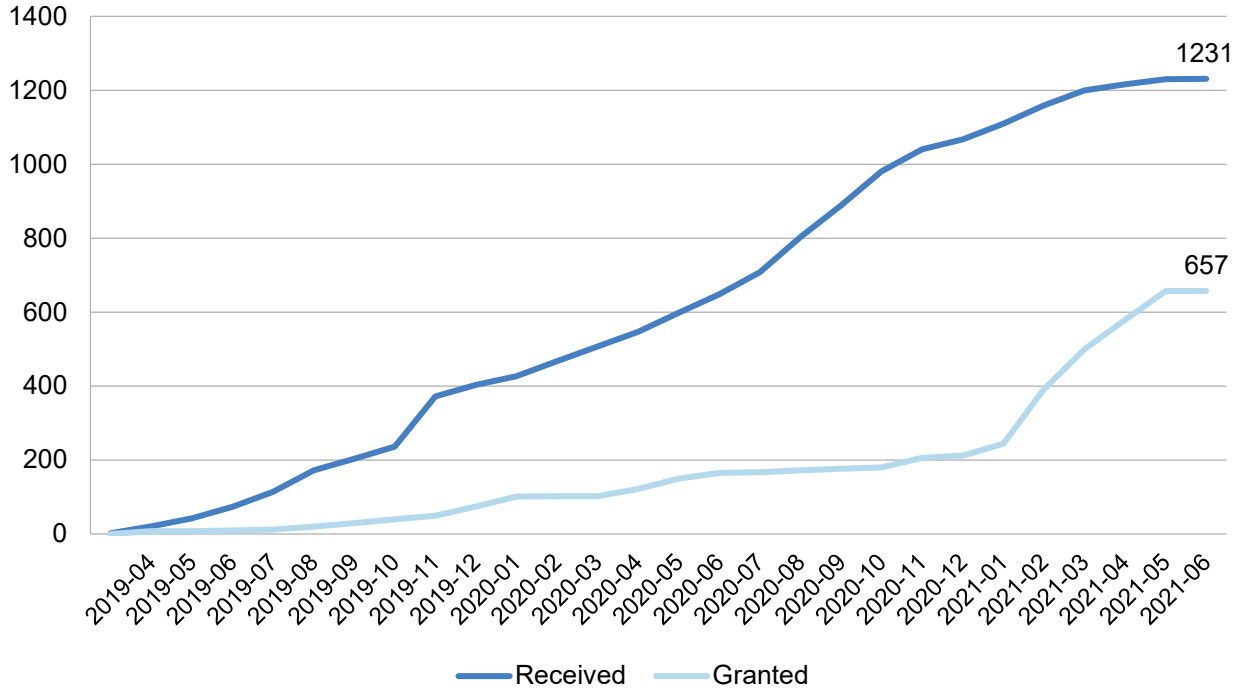
2.37 Figure 2.2 illustrates DISP applications received and granted each month between April 2019 and June 2021. Of the 1267 applications received as at 8 June 2021, 657 DISP memberships had been granted, 591 applications were awaiting processing and 19 applications had been withdrawn by the applicant.

40 For example, in 2020 two separate industry entities wrote to the Minister for Defence and Minister for Defence Industry to express concern about delays in processing their DISP membership applications and the possibility that the delays could place them at risk of losing contracts.

41 The April 2019 announcement was made by the Minister for Defence Industry as part of a DISP reform initiative. Defence advised the Secretary of Defence and the Chief of the Defence Force in October 2018 that:

> There are currently 571 active DISP company members, many with multiple contracts and separate DISP memberships. Under the DISP reforms we anticipate a significant increase to these numbers, which, based on information in the 2016 Defence Industry Policy Statement, could be as high as 3000 new companies likely to join DISP. We anticipate the majority of new applicants will seek entry level DISP membership, which will require limited resourcing on behalf of Defence through a self-service model being implemented.

Figure 2.2: Applications received and granted – cumulative total from April 2019 to June 2021



Note: Defence advised the ANAO in June 2021 that it: 'does not have records of processing rates for DISP applications prior to April 2019, noting the limitations of the DISMS system then in use'.

Source: Defence data.

2.38 Of the 591 applications awaiting processing as at 8 June 2021:

- 219 were in 'active uplift', where Defence places the applicant in an uplift program to improve their security maturity (see Box 2);
- 49 were inactive. Defence deems applications inactive where an entity has not provided the required information to Defence for their application to be processed, and has not responded to further communication from Defence for over 75 days;
- 13 were 'paused'. Defence pauses processing of an application when it is waiting for the applicant to provide a completed application pack, and the entity has not responded to further communication from Defence for over 60 days;
- 38 were yet to be assigned to a processing officer[42]; and
- 272 were actively being processed by Defence.

2.39 Box 2 (below) provides further information regarding Defence's application of 'uplift'.

42 This includes applications that are currently still in 'triage' or assessment for completion of forms and appropriateness of DISP level applied (with supporting evidence).

Box 2: 'Uplift' approach to DISP membership applicants

Defence advised the ANAO that DISP membership applicants who do not meet the required security standards to be granted DISP membership are 'placed into an uplift program to improve their level of security maturity'.

The uplift approach is referenced in Defence's communication materials for industry on its external website, but is not documented in the DSPF Control 16.1 – Defence Industry Security Program. Defence advised the ANAO that the 'uplift program' is a broad term used to describe the process where it informs the industry entity of the specific improvements to its security arrangements in order to meet the requirements for, and therefore obtain, DISP membership.

Defence advised the ANAO that as at 28 May 2021, 218 DISP applicants had not met the required security standards to be granted DISP membership, and were undergoing 'uplift'.

Defence further advised the ANAO that 'Defence is not able to oversee every contract and at this stage Defence is not able to assure that the entities in the uplift pool are not being engaged.'

In the absence of Defence systems that identify whether a contract requires DISP membership, it is not possible to determine whether Defence has entered into contracts that require DISP membership with entities that have not been granted membership, and are in the uplift program.

Source: ANAO analysis of Defence documentation.

Timeframes for processing applications

2.40 Defence's external DISP website outlines the expected processing times for DISP applications (see Table 2.1 below).

Table 2.1: Expected timeframes for processing DISP applications by membership level as advised to industry by Defence

Membership level	Industry entity's security status at the time of application	Timeframe to process DISP membership
Entry level	The industry entity has all the required clearances and certifications.	2–3 months
Levels 1, 2 and 3	The industry entity has all the required clearances, certifications and accreditations.	4–6 months
All levels	The industry entity does not have all the required clearances, certifications and accreditations.	Depends on the business' level of security maturity

Source: Defence external DISP website: https://www1.defence.gov.au/security/industry/how-apply#How [accessed 27 January 2021].

2.41 Defence further advises on its external website that: 'timeframes for processing DISP membership vary based on the required level of membership, current level of security maturity and requirements and dependencies on internal Defence resources'. Defence informed the ANAO in June 2021 that 'timeliness for processing DISP membership also depends on the complexity of the application, and responsiveness of the entity'.

2.42 Defence informed the ANAO in December 2020 that it is yet to develop key performance indicators for processing timeframes for DISP membership applications. In early February 2021, in the course of this audit, the First Assistant Secretary, Defence Security and Vetting Service, advised the Associate Secretary of Defence that DISO intends to set benchmark timeframes for all membership levels once the application backlog is reduced by May 2021. In June 2021, Defence informed the ANAO that 'DISO is developing key performance indicators in the establishment of BAU pace of activity, as the backlog of applicants has been substantially reduced'.

2.43 The ANAO reviewed the actual processing times for the 219 memberships granted as at 18 January 2021. For the 219 membership applications reviewed:

- the shortest processing time was two days;
- the longest processing time was 534 days (17.8 months)[43]; and
- the average processing time was 198 days (6.6 months), with a median processing time of 175 days (5.8 months).

2.44 Between January and June 2021, the average and median processing time for DISP membership applications was around 11 months. The increase in timeframe for processing applications could be attributed to Defence's activities to reduce the application backlog including processing a large number of outstanding DISP membership applications received in 2019 and 2020 (see paragraphs 2.52 to 2.57).

2.45 For the 657 memberships granted to June 2021, the application processing time by DISP membership level is set out in Table 2.2 below. The cells shaded grey reflect applications processed within the timeframes advised to industry as set out in Table 2.1 above.

Table 2.2: Application processing time by DISP membership level[a]

Processing Time[b]	Entry level No. applications	Level 1 No. applications	Level 2 No. applications	Level 3 No. applications
Less than 3 months	15[c]	8[c]	20[c]	15[c]
Between 3 and 6 months	27	25[c]	25[c]	24[c]
Between 6 and 12 months	73	68	72	59
More than 12 months	27	118	37	44

Note a: The table includes the governance security level applied for by the DISP applicant. DISP members can apply for different levels for each security element: governance, physical, personnel, and ICT/cybersecurity.

Note b: Measure of month is 30 calendar days.

Note c: Applications processed within the timeframes advised to industry as set out in Table 2.1 above.

Source: ANAO analysis of Defence data.

43 This was for a DISP membership application that included level 3 governance.

Prioritisation of applications for processing

2.46 In January 2021 Defence commenced processing DISP applications based on four priority categories (a triaging approach). In order of priority, these categories are:

1. where an industry entity has a contract with Defence to support an ongoing Defence operation[44];
2. where an industry entity has a contract with Defence;
3. where an industry entity is planning to tender for a Defence opportunity, or in negotiations for a Defence opportunity; and
4. where an industry entity is applying for DISP with no existing relationship with Defence and no immediate tender opportunities.[45]

2.47 Table 2.3 below shows, as at 18 January 2021, the number of: DISP applications by priority category; memberships granted by priority category; and applications which remain unprocessed, by priority category.

Table 2.3: Number of DISP applications by priority category as of 18 January 2021

Priority category	Total applications	Memberships granted	Unprocessed applications
1	428	165	263
2	266	19	247
3	113	14	99
4	285	21	264
Total applications	**1092**	**219**	**873**

Note: Unprocessed refers to applications that Defence has not yet processed and applications that Defence has commenced processing.

Source: Defence data.

44 Defence advised the ANAO in August 2021 that: 'The DISP Application Form AE250 asks applicants to declare the current Defence contracts requiring DISP membership and requests the entity provide the details for each contract, including the project names, number, classification, start and end dates and the Defence project or contract manager's name and contact details. Defence uses this information to verify DISP requirements with contract managers.' Defence further advised that: 'Contract Managers use the Notification of Engagement Requiring DISP Membership, form AE250-2, to advise DS&VS about the entity Defence is engaging with; details of the contract/panel/partnership; and the security requirements of the contract/partnership including DISP membership levels. Receipt of this form triggers the prioritisation of a DISP membership application. Defence will improve visibility of all contracts held by an entity with Defence, by amending the AE250 to require entities to confirm a complete list of contracts on application'.

45 Defence advised the ANAO in August 2021 that: 'Category 1 refers to industry entities engaged in a contract with Defence to provide direct support to an ADF Operation (domestic or international)' and that 'Category 2 refers to industry entities engaged in a contract with Defence for any purpose other than direct support to ADF operations'. Defence further advised that: 'In addition to the broad categories, in January 2021, a further prioritisation framework was established to assist in eliminating the backlog of applicants. The assigned priority guides DISP processing officers and provides an indication of the expected processing times: The priorities are: P1 – Shipbuilding related entities, Universities; P2 – Applications older than 12 months, Transitioning members; P3 – Have current contract; P4 – Have no current contract'.

2.48 Table 2.3 shows that as at January 2021, 510 DISP applicants categorised as priority 1 and 2 (those with existing contracts with Defence) had not yet been granted DISP membership.[46] Defence advised the ANAO in June 2021 that:

> The 510 unprocessed priority 1 and 2 DISP applicants as at January 2021 were at that stage not granted DISP membership and a DISP suitability assessment had not been completed. Defence requires security policy to be adhered to in contracts. Any breach or incident must be reported.
>
> Assurance of adherence to the DSPF is conducted through DSPF and PSPF annual reporting. Control Owners may conduct additional assurance activities related to contract performance.[47]

2.49 Defence further advised the ANAO in June 2021 that:

> Prior to January 2021, there was no effective prioritisation of DISP resources against DISP applications received. Post January 2021, a priority framework was implemented and DISP applications were assigned to DISP case officers on a priority basis. Case officers were then tasked to process applications in priority order.

2.50 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 510 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 — that is, the entity holds a contract with Defence to support an ongoing Defence operation.

2.51 The Defence Security and Vetting Service informed the ANAO in February 2021 that it is seeking internal approval for a new IT system to process and manage DISP membership applications. The proposed system is discussed in Chapter 3.

Application backlog — resolution activities

2.52 As part of tranche 1 of the DISP Improvement Program[48], Defence aims to improve overall processing timeframes and reduce the current backlog of applications. In November 2020, Defence advised the Minister for Defence Industry on the status of the DISP program as follows:

> … Defence did not allocate resources to meet the new program demand or other broader reforms, despite an expected growth in memberships from an existing pool of 600 to an estimated 5,000. The combined lack of resources, immature processes, and insufficient Defence awareness of DISP has inevitably led to application delays and inefficiencies managing DISP.

---

46 A number of these applicants may have been granted DISP membership prior to April 2019. However, DISP membership granted prior to April 2019 was no longer valid as of April 2021 (see paragraph 2.31).

47 The Australian Government's Protective Security Policy Framework (PSPF) requires all non-corporate Commonwealth entities to report annually to their Minister and the Attorney-General's Department to provide assurance about their implementation of sound and responsible protective security practices, and to identify security risks and vulnerabilities and the steps being taken to mitigate them. In Defence, this annual reporting is underpinned by annual reporting by Defence Control Owners (an SES or ADF Star Rank Officer) assigned accountability and authority to manage a specific Defence security risk, as identified in the Defence Security Principles Framework (DSPF). Control Owners are required to provide an annual report to the Defence Security Committee on each security risk they are responsible for.

48 See Figure 1.1.

2.53 In February 2021 the First Assistant Secretary, Defence Security and Vetting Service, requested additional resourcing from the Associate Secretary of Defence to address the backlog of DISP membership applications. The Associate Secretary was advised that a number of improvements had been implemented to address the application backlog, including:

> a. Triage capability: since 1 December 2020, we are triaging applications to ensure they are complete, and to assign a dedicated processing officer and level of priority.
>
> b. Processing surge: to process more applications the processing capacity has been supplemented through AGSVA's vetting surge capabilities and redirecting analysts and security service teams to conduct more physical certification, accreditations and foreign ownership, control and influence (FOCI) checks.
>
> c. Governance: strengthening DISP management and support structures, including a new EL2 to lead the development and implementation of a customer relationship management program, and remove the risk of running the program off an Excel spreadsheet. This will aid data collection, data integrity, reporting and processing.
>
> d. Performance indicators: developing DISP process Key Performance Indicators (KPIs) and Service Level Agreements (SLAs) with our dependent functions to improve delivery timeframes.

2.54 The First Assistant Secretary, Defence Security and Vetting Service, further advised the Associate Secretary that:

> In January 2021, we achieved 41 DISP membership application approvals (representing a 310% increase over the previous monthly averages). With the surge capacity in place to focus on erasing the backlog by the end of February, we are working to complete all Entry Level application approvals within a benchmark timeframe of 30 days. We will then work to set benchmark timeframes for all membership levels.

2.55 In March 2021, Defence advised the Minister for Defence Industry that:

> We are on track to reduce the current backlog by May [2021], enabling us to maintain an inventory of approximately 150 applications ongoing assurance checks. We will be well placed to service demand and complete more applications than we receive each month, thus preventing a backlog reoccurrence.

2.56 Defence informed the ANAO that:

> As at 28 May 2021, of the 1144 eligible DISP applications received (entity has provided DISO with all requested paperwork): 659 membership have been granted; 218 are currently being supported to meet DISP entry requirements; with the remaining 267 currently undergoing the required security assessment/checks.

2.57 From January 2021 to June 2021, Defence increased its rate of processing DISP applications. With a surge capacity in place[49], Defence records indicate that it has processed twice as many applications in this six month period (445 applications granted) compared to the previous 21 month period (April 2019 to December 2020) when 212 applications were granted.

49 See Table 2.1 for expenditure and staffing levels for managing the DISP in 2019–20 and 2020–21.

3. Monitoring compliance with contracted DISP requirements

Areas examined
This chapter examines whether Defence has established and implemented fit for purpose arrangements to monitor compliance with contracted DISP requirements.

Conclusion
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.

Areas for improvement
The ANAO made three recommendations aimed at improving DISP assurance processes and supporting documentation.

3.1 This chapter examines whether Defence has established and implemented fit for purpose arrangements to monitor compliance with contracted DISP requirements. The ANAO examined:

- the monitoring and assurance activities that had been established by Defence to assess industry entities' compliance with contracted DISP requirements; and
- how Defence's contract managers were made aware of the outcomes of DISP compliance monitoring and assurance activities, to inform the effective management of contracts with DISP requirements.

3.2 As outlined in Table 1.1, the Defence Security and Vetting Service (DS&VS) is responsible for administering the DISP, through its Defence Industry Security Office (DISO). Defence contract managers are responsible for assessing and managing project security risk. Defence contract managers therefore have a shared responsibility, with the contracted parties, for monitoring and ensuring compliance with the security risk management arrangements in contracts.[50]

50 As discussed in Chapter 4, where a contractor, who is a DISP member, does not comply with the security responsibilities and obligations outlined in the DSPF and required under the contract, contract managers may issue a contract notification. In February 2021, Defence advised the ANAO that Defence Security and Vetting Services had not received any breach of contract notifications in relation to DISP members.

Has Defence established effective monitoring and assurance processes to assess compliance with contracted DISP requirements?

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.

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.

3.3 To effectively monitor compliance with contracted DISP requirements, Defence needs to be able to identify which of its current contracts:

(a) must, in accordance with the Defence Security Principles Framework (DSPF), require the contracted entity to hold DISP membership; and

(b) include such a requirement.[51]

3.4 To assess whether Defence has established effective processes to monitor compliance with contracted DISP requirements, the ANAO examined if Defence has:

- a complete and accurate list of existing contracts that include DISP requirements;
- assurance mechanisms in place to confirm that DISP clauses are included in contracts as required;
- a fit for purpose system to maintain DISP membership records; and
- a compliance and assurance framework in place to assess industry entities' compliance with DISP requirements.

Completeness and accuracy of Defence's list of contracts with DISP requirements

3.5 Defence was unable to provide the ANAO with a complete and accurate list of Defence contracts with DISP clauses.

3.6 As discussed in paragraph 1.30, for the purposes of audit sampling, the ANAO sought from Defence a list of current contracts that included a clause requiring the contracted industry entity to hold DISP membership. In response to the ANAO's request, Defence developed a spreadsheet of

51 The contract is the means by which Defence sets out the specific responsibilities of the contractor to comply with the minimum standards for the protection of security classified information, as detailed in the security policy framework in place at the time the contract was entered into. Since at least 1978, Defence security policy has required contracted entities to be members/participate in the DISP, when responsible for handling sensitive and classified information. However, it has not always been mandatory for Defence contract managers to include a DISP membership clause in the contract where DISP membership is required. Defence introduced this mandatory requirement through amendments to the Defence Security Manual effective 31 October 2014.

contract data by cross-referencing the Australian Business Numbers of current DISP members[52] with AusTender data. Table 3.1 below provides a summary of DISP contract data Defence provided to the ANAO in November 2020.

Table 3.1: Number and value of contracts with DISP members (granted membership since April 2019) — July 2018 to November 2020

Category	Total Defence Contracts[a]	Contracts held by DISP members (granted membership since April 2019)
Number of Contracts	58,310	6,872 (11.8 per cent)
Value of Contracts	$64.8 billion	$22.7 billion (35 per cent)

Note a: The figures in this column differ from the figures of 16,503 active contracts with a total commitment of $202.4 billion as at 24 March 2021 (see paragraph 1.1). The figures in paragraph 1.1 represent all active contracts in Defence as at 24 March 2021, while the figures in Table 3.1 represent total Defence contracts between July 2018 and November 2020.

Source: Defence.

3.7 The data provided by Defence was assessed by the ANAO as being neither a complete or accurate representation of the contracts that included DISP clauses, because:

- The data may include contracts held by a DISP member, where there may not be a DISP requirement clause. That is, Defence was unable to filter the data to show contracts with DISP clauses and without DISP clauses.
- The data only includes contracts with DISP members that had been granted membership since April 2019. At the time the data was collated Defence records indicated that there were a further 312 entities with DISP memberships granted prior to April 2019 that had active Defence contracts.
- AusTender data does not include contracts below $10,000 nor contracts that have a high level of security classification.
- The data does not include contracts that include a DISP membership clause but the contractor has not been granted, or applied for, DISP membership.

3.8 A review of DISP membership records undertaken by DISO in 2019 identified shortcomings in Defence's contract management practices and record keeping, including instances of Defence contract managers failing to:

- maintain accurate records of active projects and contracted industry entities;
- adhere to Defence security policy requirements;
- communicate contract changes (for example, commencements, extensions and closures) across Defence functions; and
- confirm DISP membership before engaging industry entities in security classified projects or activities.

52 For DISP memberships granted since April 2019.

3.9 The 2019 review was unable to obtain accurate records of all Defence contracts involving DISP members or applicants. The review was limited to industry entities for which Defence had DISP membership data, and the report stated that it was likely that Defence had many contracts with DISP requirements that were not visible to Defence's Security and Vetting Service.

3.10 ANAO testing confirmed that Defence does not have a source of relevant contract data to support DISP assurance activities, nor does it capture information about DISP membership requirements in contracts in any of its corporate systems that hold contract or supplier data.[53]

3.11 The Defence Security and Vetting Service has identified the following high level requirement for a DISP Customer Relationship Management System, for which it is seeking internal approval (discussed further in paragraphs 3.32 and 3.64):

> At every stage in the assessment and review of a DISP entity, information regarding the contracts the entity has with Defence is critically important. The number, value and nature of these contracts impacts the level of risk the entity poses to Defence and the type of controls that must be in place to manage that risk.

Assessment of DISP membership requirements in Defence projects audited by the ANAO since July 2019

3.12 The ANAO, in the course of its audit work, has had access to a number of contracts that Defence has established with industry. As Defence was unable to provide a complete and accurate list of Defence contracts with DISP clauses, the ANAO examined whether the threshold DISP requirement relating to DISP membership had been met in four contracts from recent performance audits. The four contracts reviewed by the ANAO were the:

- Offshore Patrol Vessels Acquisition Contract (signed 31 January 2018) with Luerssen Australia Pty Ltd.
- Land 400 Phase 2 Combat Reconnaissance Vehicles Acquisition Contract (signed 9 August 2018) with Rheinmetall Defence Australia Pty Ltd.
- Submarine Design Contract (signed 1 March 2019) with Naval Group Australia.
- Evolved Cape Class Patrol Boat Acquisition Contract (signed 30 April 2020) with Austal Ships Pty Ltd.[54]

3.13 DISP membership was a requirement in each contract. In respect to the four contracts, two of the prime contractors (Naval Group and Rheinmetall Defence Australia Pty Ltd) have held DISP membership since the contract was signed, and one (Luerssen Australia Pty Ltd) obtained membership nearly 3.5 years after the contract was signed. Defence records show that Austal Ships Pty Ltd has applied for, but not yet been granted, a new DISP membership. Austal was previously

53 At present the only way to confirm that DISP requirements are included in required Defence contracts would be to manually check each contract.

54 The ANAO performance audits that examined these contracts are: Auditor-General Report No.12 2020–21 *Defence's Procurement of Offshore Patrol Vessels — SEA 1180 Phase 1*; Auditor-General Report No.18 2020–21 *Defence's Procurement of Combat Reconnaissance Vehicles (Land 400 Phase2)*; Auditor-General Report No. 22 2019–20 *Future Submarine Program – Transition to Design*; and the in progress audit of Defence's procurement of six evolved Cape Class patrol boats due to table at the end of 2021.

granted DISP membership in August 2001. Appendix 7 sets out the results of the ANAO's review of compliance with the DISP membership requirements in the four contracts.

Assurance mechanisms to confirm that DISP clauses are included in required contracts

3.14 Defence advised the ANAO that it does not have any specific mechanisms in place to provide assurance that the appropriate 'core' DISP contract clauses are included in Defence contracts that require DISP membership under Defence security policy. Defence is therefore not able to provide complete and accurate information on the number or value of these contracts that have, or should have, a clause for DISP membership.[55]

3.15 Further, notwithstanding the findings of Defence's limited scope Defence Industry Security Management System (DISMS) remediation activity[56], there is no evidence that Defence has subsequently checked, or assessed the risk, across its population of current contracts, that industry entities are accessing security classified information and assets without holding the appropriate levels of DISP membership.

3.16 The ANAO analysed the 1,092 applicant entries in Defence's DISP Master Spreadsheet as at 18 January 2021, and matched 873 applicants who had not yet been granted DISP membership with AusTender contract notices between July 2018 and December 2020. The ANAO found that:

- 419 of the 873 DISP applicants (48 per cent) had 20,460 contracts with Defence with a value of $22 billion.
- Of these 20,460 contracts, 770 (with a value of $3.3 billion) had a confidentiality flag[57] indicating confidential subject matter or a contract that is producing a confidential output.

3.17 While not all of these contracts may require DISP membership in accordance with the DSPF, Defence does not have an assurance mechanism in place to check that these contracts have a clause for the contractor to hold DISP membership. Defence therefore has limited assurance that security classified information and assets are accessed only by industry entities with the appropriate levels of DISP membership. Further, a Defence review has identified that the risk of industry entities accessing highly security classified information and assets without DISP membership has been realised (this is discussed further in paragraphs 4.10 and 4.11).

3.18 With limited visibility of the population of contracts that include DISP memberships (as discussed above) and no specific assurance mechanisms in place to assess whether, where required

55 Defence advised the ANAO in October 2020 that DISO audits against the requirements of the DISP, which is set out in Defence security policy (DSPF). DISO does not audit against contractual requirements. Defence further advised that each domain has a compliance and assurance function which undertakes assurance and compliance testing on the management of contracts.

56 Through this 2019 and the 2020 review activity, discussed further in paragraph 3.24, Defence concluded that it had a systemic problem with maintaining accurate records in DISMS.

57 Entities are required to identify (flag) on AusTender whether a contract includes confidentiality provisions. Advice on the process is provided by the Department of Finance at: https://www.finance.gov.au/government/procurement/buying-australian-government/confidentiality-throughout-procurement-cycle%23awarding-a-contract [accessed 26 July 2021]. A confidentiality flag is self-reported by the responsible entity. The ANAO included contracts with confidentiality flags as an indication of contracts that may involve sensitive information, and therefore may require a DISP clause.

by Defence policy, the mandatory clauses for DISP membership are included in current Defence contracts, Defence is constrained in its ability to gain assurance that:

- all Defence contracts that should include a clause requiring the contracted industry entity to hold DISP membership, do so in accordance with the Defence Security Principles Framework[58];
- contracted entities hold the appropriate DISP membership levels for their contract/s with Defence[59]; and
- security classified information and assets are being accessed only by contracted entities with the appropriate levels of DISP membership.

3.19 Defence identified this limitation in its data in November 2019 and has not yet addressed it.

3.20 As Defence has identified DISP as a security risk control under the DSPF, there would be benefit in Defence establishing the means to obtain assurance that DISP requirements are met for all active contracts. There would also be benefit in Defence reviewing its current contracts to determine if DISP requirements have been met.

Recommendation no. 3

3.21 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.*

Tracking DISP memberships

3.22 Defence requires complete, accurate, and readily accessible records of DISP members to effectively assess contracted entities' compliance with contracted DISP requirements. During this audit, Defence stored its DISP membership records across two information management systems (see Table 3.2 below).

58 As at December 2020, Defence had published some 70,200 Contract Notices on AusTender with a contract end date of July 2018 or later, and had some 16,300 contracts 'on foot' at that time. Defence published 85,051 contracts on AusTender between 1 July 2017 and 31 December 2020.

59 Through manual data matching of Australian Business Numbers, Defence can identify which of its contracts listed on AusTender are with industry entities that have obtained DISP membership since Defence refreshed its DISP membership regime in April 2019. However, due to limitations in Defence's contract data discussed above, any such listing does not allow a comparison of the DISP membership levels required by the contracts with the DISP membership levels held by the industry entity. Such a comparison requires a manual review of each Defence contract.

Table 3.2: DISP membership record systems

Defence Industry Security Management System (DISMS)[a]	DISP master spreadsheet
• Contains membership records for DISP applications received by Defence prior to 1 April 2019.[b] • Microsoft SQL Server Database. • As at October 2020, contained the data associated with 549 'active' DISP memberships granted prior to 1 April 2019. • In June 2021, Defence advised the ANAO that DISO had ceased using this system and that it was decommissioned in 2020.	• Contains membership records for DISP applications received by Defence after 1 April 2019.[b] • Microsoft Excel-based spreadsheet. • As at 8 June 2021, contains the data associated with 1,230 DISP membership applications, from which Defence has granted 657 DISP memberships.

Note a: Between August 2019 and October 2020, Defence reviewed its DISP membership data stored in the DISMS. Some of the findings are discussed in the paragraphs below.

Note b: As discussed in Chapter 2, in April 2019 Defence opened DISP membership to any Australian corporate entity that wishes to apply, and not just entities with an existing Defence contract.

Source: Defence documentation.

Reviews of DISP membership data

3.23 Between August 2019 and October 2020, Defence reviewed DISP membership data stored in the Defence Industry Security Management System (DISMS).[60]

3.24 The review identified completeness and accuracy issues for the validity of over 900 DISP memberships for current contracts and subcontractors providing a range of services to Defence, including security vetting, psychological assessments, and outsourced security guard services to Defence sites nationally.[61] Defence identified 'significant data quality issues that had been on-going for over a decade' and that the 'DISMS was poorly maintained and administered, resulting in significant issues with data integrity, confidentiality and accessibility'. Through this review activity, Defence concluded that it had a systemic problem with maintaining accurate records in DISMS.

3.25 In December 2019, Defence reported to the enterprise-level Defence Security Committee that the data remediation activity had reduced the number of 'in progress' DISP applications recorded in DISMS from 131 to zero, and that it had identified and reported nine major security incidents. Defence's report from the remediation activity does not specifically identify how Defence resolved all of the 131 'in progress' DISP membership applications, however the report identifies that:

- eight applications were test applications, and were deleted;
- 13 applications had been correctly processed and required an update of the applicants' membership status in DISMS; and

60 Defence undertook two data review activities of the data in the DISMS. The first was between August and November 2019. The second was undertaken in consequence of the findings of the first activity, between June and October 2020.

61 The review's primary goal was to finalise or deny the membership applications, as appropriate. Defence reviewed 131 (12 per cent) of its 'in progress' DISP membership records stored in DISMS and identified 13 entities working on Defence activities with a security classification of SECRET or above without DISP membership or the associated security accreditation. Defence's handing of these findings is discussed in Chapter 4.

- 103 applications had discrepancies (including missing supporting documentation and lapsed contract dates), which resulted in various actions by Defence including the applications being denied, and the reporting of major security incidents.

3.26 Further, the committee was advised that: 'the remaining aspect of the data remediation projects is to confirm all 600 active (green) DISP memberships have the appropriate level of membership for the projects they are working on.'[62] Defence has since completed further work to remediate the active DISP membership data in DISMS however it did not confirm that all active DISP members in DISMS had the appropriate level of membership for the projects they are working on.

3.27 Until April 2021, the information held in DISMS remained important to Defence for identifying which DISP members had not reapplied for DISP membership by the April 2021 deadline.[63]

3.28 Defence advised the ANAO that as of 23 February 2021, 46 of the active (those with current Defence contracts) pre-reform DISP members had not applied for DISP membership under the new program. Defence further advised the ANAO in March 2021 that:

> DISO is undertaking another round of direct engagement with each of the remaining 46 companies to encourage their application into the reformed DISP. DISO will contact each listed contract/project manager to advise them of the entity's non-compliance with Defence security policy for any active pre-reform entities who fail to re-apply to the program before the deadline. Pre-reform membership will no longer be recognised after 9 April 2021, unless the entity is undergoing current DISP processing.

3.29 The ANAO requested that Defence provide a further update of the figures in paragraph 3.28. In August 2021, Defence informed the ANAO that:

> The limitations of the current spreadsheet-based tool does not enable a retrospective point in time assessment as at 10 April 2021.
>
> However, DISO can advise current details of outstanding entities under the old DISP membership. As of 09 August 2021, there are 25 entities who were sent a reminder notice by email, but have not yet applied for DISP membership.
>
> Updated status:
>
> - 25 still to apply (the list of entities will be shared with CASG [Capability Acquisition and Sustainment Group] to verify DISP requirements).
> - 21 have applied:
>   - 8 granted DISP membership
>   - 5 in uplift
>   - 6 are completing membership processing

62 The committee was not advised of the 900 DISP memberships with completeness and accuracy issues (see paragraph 3.24).

63 As discussed in paragraph 2.31, DISP members granted membership prior to April 2019 had to reapply for membership by April 2021. Defence advised the ANAO in March 2021 that pre-April 2019 membership would no longer be recognised after 9 April 2021 unless the industry entity was undergoing DISP application processing.

- 1 inactive (the entity applied but has been non-responsive for over 75 days)
- 1 withdrawn.

3.30 The ANAO also sought advice from Defence on its posture on managing contracts with DISP members whose memberships are no longer recognised. Defence advised the ANAO in June 2021 that:

> Defence relies on industry entities to provide details for current contracts. Defence relies on Defence contract managers to verify these details to support the DISP membership level being sought. As of January 2021, Defence commenced queries of AUSTENDER to also verify current contract details to support DISP membership levels being sought.
>
> DISO has conducted several data remediation activities on DISMS to ensure the transition into the new program can be as seamless as possible and any relevant gaps can be identified, and relevant measures to mitigate the risks can be implemented.
>
> One of the activities that was discussed whilst working on the 'DISP Data Remediation Project' was to "contact each listed contract/project manager to advise them of the entity's non-compliance with Defence security policy for any active pre-reform entities who fail to re-apply to the program before the deadline [9 April 2021]". Due to the lack of relevant data on DISMS, we were unable to perform this particular task.
>
> Instead, multiple steps were taken to contact all extant members from the 'old DISP program' over the two year transition period, with a reminder to re-apply to the then 'new DISP'. A dedicated team was assigned to contact all DISP members listed in DISMS, and to provide any support to entities that re-applied as a direct result of the outreach activities.

3.31 In July 2020, a review (by Synergy Group Australia) into Defence's management of the DISP stated that Defence's systems for managing DISP memberships are not fit for purpose and that this carried risk associated with the ongoing confidentiality, integrity and availability of the data. In February 2021, the First Assistant Secretary, Defence Security and Vetting Service, advised the Associate Secretary that DISO is 'missing all or most of the capability' necessary for effective DISP information management and reporting'. Appendix 6 provides a summary of DISO's required capabilities as advised to the Associate Secretary in February 2021.

3.32 As discussed in paragraph 3.11, the Defence Security and Vetting Service is seeking internal approval for a DISP Customer Relationship Management System. It plans to address the issues identified with its management of DISP membership through the development of that IT system, which is discussed further in paragraph 3.64. In June 2021, Defence informed the ANAO that:

> Delays in achieving Gate 0 and 1 approvals will impact the implementation date for the CRM. The current projection is for an Interim Operation Capability to be deployed in late January 2022, but this is likely to slip further.

Availability of DISP application records

3.33 The ANAO requested the following documentation for contracts with a DISP requirement, or for contractors with DISP membership for the last two years:

- completed forms notifying DISO that a contract contains a DISP clause;
- security incident reports;
- foreign ownership change forms; and

- contact reports.

3.34 In November 2020, Defence informed the ANAO that: 'it is likely to take weeks to get a response [to the ANAO] as this requires manual checks across thousands of documents'.[64]

3.35 In June 2021, Defence advised the ANAO that: 'Defence clarifies that all DISP-related records are stored in Objective centrally. Defence advice to ANAO was that it would take considerable time to review the over 1000 individual entity files'.

3.36 Defence's records management policy states that:

> Effective records management will support Defence in maintaining authoritative information that has integrity and is accessible, auditable, accurate, reliable, complete, and of high quality …
>
> … Defence records must be stored in a way that preserves their authenticity, reliability, discoverability, accessibility, quality, usability, and security for as long as needed.

3.37 The difficulty encountered in accessing DISP membership records, and the inaccuracies observed in forms recording contracts' DISP membership requirements, is inconsistent with the aims and expectations of Defence's records management policy and raises questions regarding the quality of the data used to support Defence's targeted assurance activities for DISP and the veracity of the upwards reporting to the Defence Security Committee (discussed in paragraph 3.57).

Recommendation no. 4

3.38 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.*

Compliance and assurance framework to assess industry entities' compliance with DISP requirements

3.39 A key purpose of the DISP is to provide Defence with assurance that industry entities are effectively managing security risks (see paragraph 1.5). To obtain this assurance, Defence requires efficient and effective processes and systems for monitoring compliance with contracted DISP membership requirements.

3.40 Defence informed the ANAO in February 2021 that despite the DISP being a long running program spanning several decades, prior to the establishment of DISO in August 2019 there was no assurance framework in place.

3.41 As discussed in Chapter 1, a 2017 review made six recommendations relevant to the DISP. One of the recommendations was that Defence 'enhance security assurance to assess DISP

64 For example, Defence advised the ANAO that the DISP application forms 'are individually stored in each applicant's objective folder'. Objective is Defence's electronic records management system. Defence further advised that 'DISO potentially holds hundreds of AE250-2 forms, many of which may not provide accurate information regarding a contract's DISP membership requirements' and that 'should the ANAO require the manual collation of these documents, it will likely take weeks to collate these documents'. AE250-2 forms are provided to DISO by Defence contract managers notifying of a contract that contains a DISP clause.

members' security performance and compliance with self-reporting obligations'. At the direction of the Australian Government, Defence established DISO in August 2019 to undertake these and other functions.

3.42 In February 2021, the First Assistant Secretary, Defence Security and Vetting Service, assessed and advised the Associate Secretary that DISO is 'missing all or most of the capability' for DISP assurance, including for risk-informed reassessments of approved participants to confirm ongoing suitability and capability, cyber assessment and independent risk assessment revalidation for members with DISP security levels 1-3, and targeted deep dives.

3.43 In July 2020, a review (by Synergy Group Australia)[65] of Defence's management of the DISP had assessed that:

- whilst the DISP participation application and initial assessment process has been in place for several years, ongoing assessment and assurance of participants of their ongoing suitability is less mature;
- initial DISO 'audit' results indicate DISP participants are not managing Defence's security risk in accordance with the DSPF or to the standard required[66]; and
- Defence has few mechanisms in place to provide adequate assurance that industry entities are complying with DISP obligations.

3.44 Defence advised the ANAO that it is seeking to address these issues as part of its DISP Improvement Program. In June 2021, Defence advised the ANAO that:

> As part of the implementation of the DISP Improvement Program, Defence has brought forward the planned Tranche 2 activity 'DISP Assurance Model'. The DISP assurance model was developed from April to June 2021 and describes the integrated assurance framework for DISP members through application and membership stages. Key components of the membership assurance model include:
>
> - An Annual Security Report assessment process (implemented).
> - A risk-based methodology for selecting members for more active assurance review: Ongoing Suitability Assessment and 'deep-dive' audit (implemented).
> - An Ongoing Suitability Assessment (OSA) process that forms the basis of regular, 'rolling', assessment of continued compliance with DISP requirements (currently being piloted with initial group of 10 DISP members). It is anticipated the OSA pilot will be completed and move into full implementation in the September 2021 quarter.
> - Deep-dive audits of those members identified as meeting key audit criteria (implemented, with 2021/22 audit plan undergoing final approval by CSO).
>
> Ongoing improvement and enhancement of these assurance activities will be developed as a part of the analysis and continuous improvement activities in DISO.

65 Defence records indicate that Synergy Group Australia applied for DISP membership in June 2019 and was granted DISP membership in December 2020. The ANAO confirmed that the contract with Synergy Group Australia did not have a requirement for DISP membership.

66 As noted in Table 3.3, these reviews include stakeholder interviews and examination of supporting documentation. The reviews do not test an entity's security controls or comply with auditing standards.

3.45 Defence's current assurance framework for the DISP, as set out in the Defence Security Principles Framework (DSPF)[67], comprises five core elements supported by five categories of assurance activities. Table 3.3 below sets out, as at August 2021: the activities undertaken for each element; and a summary of the ANAO's assessment of Defence's current assurance activities for the DISP against the approved assurance framework in the DSPF control document. In summary:

- Defence does not have a detailed implementation plan for how it will implement the DSPF requirements.[68]
- The assurance activities conducted to date provide limited assurance in regards to the four entities that have been reviewed to date[69], and no assurance in regards to the entire population of DISP members.

67 On 2 July 2018, the DSPF replaced the Defence Security Manual as the primary source of Defence security policy.

68 As discussed in paragraph 1.24, during its inquiry into Australian Government Security Arrangements, the 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. The report on the JCPAA's inquiry noted that:

> The Committee questioned Defence on who was responsible for conducting the audits and how they are verified, but was unable to ascertain a clear answer from Defence. Defence gave the Committee assurances that the companies were reporting that they are cyber resilient, but was unable to explain what compliance mechanisms were in place to verify the reporting is accurate and meets the mandated standards.

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)*, p. 24, available from: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/PersonnelSecurity [accessed 13 July 2021].

69 The four entities are: Sigma Bravo, Boeing Defence Australia, CEA Technologies, and Key Vetting Services.

Table 3.3: Defence's DISP assurance framework as at March 2021 and updated as at August 2021

Defence Security Principles Framework (DSPF) core element and supporting activities	Defence's assurance activities as at March 2021 and updated as at August 2021	Summary of the ANAO's assessment of Defence's implementation as at August 2021
Compliance with DISP eligibility and suitability requirements Assurance and compliance activities undertaken by Defence Industry Security Office (DISO)	As at March 2021, Defence had completed reviews (called 'deep dives') of four DISP members to assess compliance against the DISP requirements in the DSPF since DISO was established in August 2019. • The deep dives included stakeholder interviews and, for three of the four, an examination of supporting documentation. • The deep dives did not test the entities' security controls. • Only one entity agreed to address all of the areas identified by Defence for improvement. The other three either disagreed, or partly agreed, with Defence's recommendations for improving security management. • Defence may conduct a follow up review where a deep dive determines that the contractor's security arrangements require remediation. Defence has not conducted any follow-up reviews to date. In June 2021, Defence informed the ANAO that a further five deep-dive reviews commenced during the period January to June 2021.	**Not implemented** Defence has not fully implemented the assurance activities to provide assurance that DISP members are complying with eligibility and suitability requirements. Defence informed the ANAO in November 2020 that the 'Deep Dive Audits to date were part of a DISO pilot program and were used to refine templates and processes. These completed audits are of varying length due to these improving processes.' As at June 2021, Defence had examined four entities, with five in the process of being reviewed[a], from over 650 members[b], to gain assurance of their compliance with DISP requirements.
Annual Security Report (ASR) Defence will review DISP members' ASRs. The DSPF states that completed ASR forms must be submitted annually within 10 business days of the anniversary of the date DISP membership was granted.	The ASR is a declaration by the Chief Security Officer of the DISP member stating that the organisation is continuing to meet the DISP eligibility and suitability requirements. Defence's membership records show that as at 18 January 2021, of the 219 DISP members granted membership since 1 April 2019, some 36 per cent of the ASRs were overdue. As at 8 June 2021, Defence records show that of the 165 DISP members granted membership since April 2019 that have had an ASR due, some 27 per cent of these ASRs were overdue. In February 2021, Defence informed the ANAO that Defence does not analyse the ASRs, but plans to use the information in these forms to inform DISO's audit program. In June 2021, Defence advised the ANAO that 'Defence does analyse the ASRs and uses the information in these forms to inform the DISO audit program'. Defence further advised the ANAO that 'Defence reviews and	**Not implemented** DISP members' ASRs are not submitted to Defence within the timeframes required. Defence has developed templates for the review of ASRs and for pursuing overdue ASRs. There is no evidence that these templates have been implemented, and no evidence of any analysis of the ASR forms.

Defence Security Principles Framework (DSPF) core element and supporting activities	Defence's assurance activities as at March 2021 and updated as at August 2021	Summary of the ANAO's assessment of Defence's implementation as at August 2021
	assesses the ASRs against the ongoing suitability requirements for DISP membership', and that 'these assessments inform the DISO audit program'.	
Intelligence led assurance program including: • random and targeted security checks of DISP members; • assessment of industry security incident, fraud and contact reports; and • conduct security investigations as appropriate.	Defence advised the ANAO that between 1 January and 30 November 2020, DISP members reported 294 security incidents to Defence's Security Incident Centre. Defence categorised 172 of these incidents as 'major' and 122 as 'minor' security incidents. One incident was investigated by Defence. Defence informed the ANAO that this was the only incident that 'met the threshold for investigation'.	**Not fully implemented** Very limited Defence analysis or investigation of security incidents reported to Defence by DISP members to identify trends and communicating these to the relevant business areas to assess and manage risks. The reports did not include information on whether the incident related to a contract that included a DISP membership requirement. No evidence of random or targeted security checks of DISP members or assessment of DISP member security incidents, fraud and contact reports to inform mitigation of the security risks.
Five year forward audit work program.	DISO has not yet developed a five year forward work program. In December 2020, Defence advised the ANAO that the COVID-19 pandemic has delayed DISO's 2020-21 audit schedule however, DISO had two audits planned for February 2021 and was in the early stages of planning a further six audits though the dates for these audits were yet to be determined. In June 2021, Defence advised the ANAO that based on Defence's 'draft DISO Deep Dive Audit Schedule' for 2021–22 Defence plans to undertake 16 audits during 2021–22, 12 of which are shipbuilding audits. In August 2021 Defence advised that: 'DISO deep dive audits are managed by Defence staff with support from contracted auditors in blended teams. DISO's audits are conducted in line with better practice audit methodologies across the audit lifecycle (planning, fieldwork and reporting). DISO uses experienced auditors to ensure that professional standards are consistent with the approach undertaken by the Institute of Internal Auditors International Professional Practices Framework (IPPF).' In August 2021, Defence further advised the ANAO that: 'An annual audit schedule provides greater flexibility to develop an audit program that is	**Not implemented** In June 2021, Defence informed the ANAO that is has 'has moved to a dynamic, annual audit schedule that is monitored throughout the year and adjusted as required to respond to changes in Defence priorities and emerging risks.' In August 2021, Defence advised that it plans to re-write the DISP policy to update the audit and assurance framework.

Defence Security Principles Framework (DSPF) core element and supporting activities	Defence's assurance activities as at March 2021 and updated as at August 2021	Summary of the ANAO's assessment of Defence's implementation as at August 2021
	responsive to emerging needs or concerns (such as those revealed through Annual Security Reports by entities), the growing DISP membership, and to take account of unexpected contingencies, such as the COVID-19 pandemic. The Audit Schedule is approved by the Assistant Secretary Security Policy & Services (AS SPS) and the Chief Security Officer.'	
Shipbuilding assurance program.	In late 2018, the Government directed Defence to undertake a cyber-assurance activity across the Shipbuilding Enterprise DISP members. In response, during April and May 2019, DISO completed what it described as 'desktop cyber-security audits' of a randomly selected sample of 19 shipbuilding DISP members to self-assess their cyber-security maturity based on a questionnaire. The report from the review also stated that the activity highlighted the limited expertise within DISO to conduct cyber audits, and it remained a key risk for the organisation. In June 2021, Defence advised the ANAO that it had commenced a total of three shipbuilding audits during April and May 2021. Defence further advised the ANAO that DISO will not develop a separate shipbuilding audit program. Instead, DISO's annual audit schedule will include shipbuilding audits.	**Not fully implemented** In August 2020, Defence informed the ANAO that: 'AS SPS as the Control Owner for Control 16.1 endorsed the decision to include shipbuilding audits in the annual audit schedule. This eliminated the need for a separate shipbuilding program to be developed. The Audit Schedule is approved by the Assistant Secretary Security Policy & Services (AS SPS) and the Chief Security Officer. The DISP policy re-write is planned to update the audit and assurance framework.'

Note a: Defence informed the Defence Security Committee that the selection of companies for its review program was based on 'the areas of risk or priority for Defence, where significant industry support is required'.

Note b: Including 312 'active' pre-April 2019 DISP members, and the 219 DISP members granted DISP membership as at January 2021.

Source: Defence documents.

3.46 As outlined in Table 3.3, Defence has made limited progress in implementing the suite of assurance activities documented in the July 2018 DSPF. Implementation remains at a very early stage, three years after the DSPF was introduced.[70]

Recommendation no. 5

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

Department of Defence response: *Agreed.*

Are Defence contract managers provided with relevant information to help manage contractors' compliance with contracted DISP requirements?

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 firms 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.

3.48 To assess whether Defence contract managers are provided with relevant information to help manage contractors' compliance with contracted DISP requirements, the ANAO reviewed if:

- DISO provides contract managers with appropriate advice regarding the findings of the assurance activities conducted on DISP memberships;
- Defence collates and shares other relevant compliance data with contract managers; and
- Defence contract managers have access to data on industry entities' DISP memberships.

DISO advice to contract managers regarding the findings of the assurance activities conducted on DISP memberships

3.49 On its external website for DISP, Defence advises that in relation to its assurance activities:

> Our audit reports are also sent to relevant Defence contract managers. These contract managers will determine whether any contractual requirements have not been met, and make a decision on whether any contractual penalties apply.

70 This was the ANAO's assessment of available evidence as at 7 June 2021. On 28 June 2021, Defence provided the ANAO with a document that sets out Defence's methodology and approach to 'DISP Ongoing Suitability and Assessment'. The document was presented 'as evidence of the ongoing assurance checks that we [Defence] now undertake'. The slide provides evidence of Defence's intent, but it is not evidence of implementation of the methodology and approach. The ANAO subsequently sought additional evidence of Defence's implementation of the methodology and approach. In August 2021, Defence provided the ANAO with a copy of an audit report template but did not provide a completed audit report to demonstrate implementation of the methodology.

3.50 In its document specifying the high level requirements for a new IT system to support the DISP[71], Defence noted that a current limitation of its tools and processes was that: 'findings from assessments and audit are not always passed through to the contract managers'.

3.51 As outlined in Table 3.3, Defence's activities to support the DISP assurance framework in the July 2018 DSPF remain at a very early stage[72], three years after the DSPF was introduced. In consequence, there is little in the way of results from these activities to date for Defence to report to its contract managers, to assist them in managing contracted DISP requirements.

3.52 There is evidence that the results of Defence's 'deep dives' of four DISP members[73] have been distributed to senior Defence leaders at the Group Head level. In June 2021, Defence informed the ANAO that it intends to provide routine reporting from its DISP compliance and assurance activities to contract managers.

3.53 In April 2020, Defence committed to biannual reporting of DISO's audit findings to the Defence Security Committee. Defence informed the ANAO in February 2021 that the biannual reporting has not occurred due to increased priority on processing DISP membership applications:

> An Audit Insights Report is currently being drafted, although it will likely be sent to DSC members 'out of session'. Priority to process DISP applications has been impacted by several factors, including developments undertaken through the DISP improvement program and COVID-19.

Collating and sharing of other relevant compliance data with contract managers

3.54 Under the DSPF, industry entities that are DISP members must report security incidents or foreign contact.[74] As part of its intelligence-led assurance program and in accordance with the DSPF, DISO is to 'assess industry security incident, fraud and contract reports'.

3.55 The 2017 review (see paragraph 1.19) found that Defence capability managers and contract managers were not consistently accessing threat information to inform project and contractual security requirements and assurance activities. In relation to security incidents, the review found that:

- data to support an enterprise-level assessment of industry security risk, such as the number and nature of DISP members and of DISP security incidents, was either not available or not reliable; and
- Defence's capacity to analyse metrics from contract and incident reports to identify trends and patterns is constrained by the limitations of existing information systems.

3.56 Defence advised the ANAO in January 2021 that DISO is notified by the Security Incident Centre[75] of security incidents involving DISP companies and that the process has been 'ad-hoc on an as-needs basis' while the Security Incidents Centre re-established monthly reporting, which was

71 The DISP Customer Relationship Management System, discussed in paragraphs 3.64 to 3.65.

72 In February 2021, Defence advised the ANAO that there was no assurance framework in place for DISP prior to the April 2019 reforms.

73 As outlined in Table 3.3, Defence has completed reviews, called 'deep dives', of four DISP members to assess compliance against the DISP requirements in the DSPF.

74 Including suspicious, ongoing, usual and/or persistent contact by a foreign national.

75 Both the Security Incident Centre and DISO are within the Defence Security and Vetting Services division within Defence.

expected to resume for 2021. The monthly reporting has not occurred. Further, Defence records provide no evidence that:

- security incidents involving DISP members have been shared with relevant contract managers;
- Defence has analysed security incidents involving DISP members to identify trends; and
- Defence communicating these trends to the relevant business areas.

3.57 Security incident data is reported quarterly to Defence's Security Committee. The data is at a high level and not categorised by DISP membership. Defence's current IT systems do not support the analysis or collation of security incident data for DISP members, and analysis of security incidents is manually intensive.[76]

Security incident data provided to DSPF control owners

3.58 As part of the 2019–20 DSPF reporting process, the Defence Security and Vetting Service provided security incident data to 'control owners' to support their assessments.[77] The data was obtained through Defence's security incident reporting forms. The results of the 2019–20 DSPF reporting process were reported to the Defence Audit and Risk Committee in December 2020. The briefing presented to the Committee stated that:

- Some control owners observed that 'the volume of security incident data provided was overwhelming'.
- The Defence Security and Vetting Service advised the Committee that it was:

  … undertaking a security incident management project where one of the deliverables will better align the security incident categories to the DSPF Controls going forward. This is expected to improve reporting and better tailor the data provided to Control Owners in the future including trend analysis, however there will continue to be a need for manual review of data to some extent.[78]

- Control owners had requested that security incidents under their controls be reported to them on a quarterly basis to support proactive review, oversight and assurance. Defence Security and Vetting Service advised the Committee that quarterly reporting was expected to be rolled out in Quarter 4 of 2020.

---

76 Defence's spreadsheet for recording DISP membership data only includes membership application data (such as company name and contact details, Australian Business Number (ABN), application date, and application priority), and does not make provision for recording security incidents or contact reports for DISP members.

77 The DSPF sets roles and responsibilities, and appoints accountable control owners to manage a specific defence security risk. There are 42 controls across 13 control owners in Defence. For the 2019–20 reporting period, of the 42 controls, two were assessed as 'embedded', 18 were assessed as 'managing', 20 were assessing as 'developing', and two were assessed as 'ad hoc'.

78 In August 2021 Defence advised the ANAO that: 'DS&VS commenced the Security Incident Reform Project in September 2019, and completed it on 3 May 2021'. Defence further informed the ANAO that: 'Key project outcomes included delivery of the new Security Report [for reporting suspicious contacts and security incidents in Defence] and updates to the DSPF Principle 77 and Control 77.1 – Security Incidents and Investigations … The smart form design of the Security Report collects information in a more efficient manner allowing for increased granularity in the available categories and sub-categories. The increased detail facilitates alignment of security incident categories to DSPF Controls. DS&VS is producing Control Owner reports on a quarterly basis. These quarterly reports commenced in Quarter 1, 2021-22 Financial Year with the report provided to Control Owners in October 2021'.

3.59 Defence advised the ANAO in February 2021 that in relation to the quarterly reporting:

> Due to the complex nature of the format of the Control Owner reporting, a quarterly frequency is not currently achievable. On final implementation of the Security Incident Reform Project (expected to be functional for the 2021–22 Financial Year) the composition of Control Owner reporting will undergo review with the aim to become more efficient allowing for increased frequency of Control Owner reporting. In the interim, monthly reports to the Group Executive Security Advisors have undergone considerable redevelopment and will be recommencing as of February 2021. The reports will be provided to each of the Group and Service's 'Executive Security Advisors' within the first two weeks of each month thereafter who will work with relevant Control Owners.

3.60 In June 2021, Defence advised the ANAO that it still did not have the capacity to produce quarterly reporting.

Contract manager access to data on industry entities' DISP memberships

3.61 As discussed in Chapter 2, implementation of the Defence Security Principles Framework relies on Defence contract managers, who are expected to include the appropriate DISP clauses in required Defence contracts. As part of this process, contract managers are required to determine what, if any, levels of DISP membership an industry entity should hold for any given contract, and include that membership requirement in the contract.

3.62 Defence contract managers do not have visibility of Defence's DISP membership data, and must request this information from the DISP administration team. Defence has identified that this adds a degree of complexity and inefficiency to implementation of the DISP that Defence is seeking to address as part of its DISP Improvement Project.

3.63 Risks relating to Defence contract managers' lack of understanding of the DISP and expectations regarding DISP membership, were highlighted in a September 2020 review by Defence internal audit (see Box 3 below).

Box 3: September 2020 internal review of Defence's collaboration with Australian universities

In September 2020, an internal review of Defence's collaboration with Australian universities found that there was an assumption by Defence contract managers that:

> … the Defence Industry Security Program (DISP) provides all the necessary assurance of appropriate security arrangements within universities. An over reliance on DISP accreditation as a key control is preventing line management from undertaking their own security due diligence as a compensating control in the absence of DISP prioritising assurance activities within universities.[a]

The review further noted that:

> There also appears to be an over reliance upon, and lack of understanding of, the DISP program by line managers. The impression formed during fieldwork was that if an university was a DISP member then the contract manager didn't have to undertake any specific security due diligence in relation to their specific relationship. Discussions with DISP management confirmed that their program is currently focused on undertaking assurance activities of DISP members within priority areas. The limited value and impact of contracts with universities on current Defence capability means that universities are not necessarily a priority for such assurance activities.

Note a: ANAO comment: under the DSPF, the Defence project manager (the definition of which includes Defence contract managers) is responsible for the security of all aspects of the project, including managing all outsourced risks. Source: Defence Security Protective Framework, Control 11 – Security for Projects, p. 10.

Source: Defence documentation.

3.64 Defence is planning to implement improvements to the information shared with contract managers through the Defence Security and Vetting Service's proposed new IT system to manage the DISP. In its document specifying the high level requirements for the new system, DISO notes that:

> The system will assist Contract Managers manage the risk of their contracts, by providing an accurate assessment of the level of security maturity of a DISP entity at a point in time, and alerts when incidents are logged or circumstances change.

3.65 In a February 2021 briefing to the First Assistant Secretary, Defence Security and Vetting Service, DISO advised that it was scoping and refining requirements for the system. In June 2021, Defence informed the ANAO that:

> Delays in achieving Gate 0 and 1 approvals will impact the implementation date for the CRM. The current projection is for an Interim Operation Capability to be deployed in late January 2022, but this is likely to slip further.

4. Managing non-compliance with contracted DISP requirements

Areas examined
This chapter examines the effectiveness of Defence's arrangements to manage identified non-compliance with contracted DISP requirements.

Conclusion
Defence has not established effective arrangements to manage identified non-compliance with contracted DISP requirements. In particular, Defence has not established an appropriate framework to manage non-compliance with contracted DISP requirements, with a clear escalation pathway. Where Defence has identified non-compliance with DISP requirements, it has not adopted a risk-based approach to compliance or pursued any of the contractual or other remediation actions available to it under the Defence Security Principles Framework.

Area for improvement
The ANAO made one recommendation aimed at establishing a documented framework for managing non-compliance with contracted DISP requirements, with a clear escalation pathway.

4.1 This chapter examines the effectiveness of Defence's arrangements to manage identified non-compliance with contracted DISP requirements. To form a conclusion, the ANAO examined:

- the framework Defence has established to manage non-compliance; and
- whether Defence has taken appropriate action when non-compliance has been identified.

Has Defence established an appropriate framework to manage non-compliance with contracted DISP requirements?

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.

4.2 Control 16.1 of the Defence Security Principles Framework (DSPF) outlines Defence's policy for managing DISP membership as a result of non-compliance with DISP requirements.

4.3 The DSPF states that:

> … non-compliance with DISP membership requirements may result in Defence downgrading, suspending or terminating an Entity's DISP membership'.

4.4 The DSPF also states that:

> Failure to comply with DISP membership requirements may have other consequences, for example:
>
> a. contractual penalties where obligations to meet a contractual requirement are not met; or
>
> b. criminal or financial penalties or sanctions under Australian law.

4.5 Defence does not have documented procedures to support its policy on non-compliance with DISP membership requirements. In July 2020, a Defence review of the DISP assessed that it has 'no clear processes for managing and escalating participant non-conformance', and identified a need for a 'documented non-compliance framework that clearly maps out escalation and sanctions for non-compliance with DISP and DSPF requirements, including deregistration'.

4.6 Defence advised the ANAO in February 2021 that it is seeking to address this issue as part of its DISP Improvement Project, and planned to develop and implement a framework for non-compliance during the first half of 2021. In June 2021, Defence advised the ANAO that:

> Defence is addressing the issue around DISP non-compliance under a policy sprint project to update DSPF Principle 16 and Control 16.1 Defence Industry Security Program.
>
> A primary focus of the policy update is to address the ambiguity around eligibility and suitability, and specify the outcomes associated with not meeting those membership requirements. We will also develop a membership denial and modification framework in line with procedural fairness principles to ensure that non-compliance is handled justly, and with integrity. As at June 2021 this is a work in progress.

4.7 There is no Defence framework to guide its officials in the management of non-compliance with contracted DISP requirements, with a clear escalation pathway. There would be benefit in Defence developing such a framework.

Recommendation no. 6

4.8 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.*

Has Defence taken appropriate action in response to identified non-compliance with its security policy?

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.

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

4.9 Defence contract managers are responsible for ensuring that industry entities hold the appropriate level(s) of DISP membership for the activities they are engaged to work on. As discussed in Chapter 3, Defence is constrained in its ability to identify non-compliance with this Defence security policy requirement. The assurance activities conducted to date provide limited assurance

in regards to the four entities that have been reviewed to date, and no assurance in regards to the entire population of DISP members (see paragraph 3.42).

4.10 Specific instances of non-compliance were identified by Defence through a limited review of pre-April 2019 DISP membership records. Defence reviewed 131 (12 percent) of the 1,112 DISP membership records between August and November 2019.[79] The review identified 13 industry entities contracted to work on Defence activities with a security classification of SECRET or above, that did not have DISP membership or the associated Defence security accreditations. Of the 13 instances:

- in nine instances, the contracts were still active and the entities had been working on the classified activities from between 16 months and 5.5 years, and in one instance possibly longer, although Defence was at the time unable to determine how long the entity had been engaged. In September 2019, the reviewer reported these nine instances to the Defence Security Incident Centre as major security incidents[80];
- in three instances the contracts were still active but did not require the sub-contractors involved to hold DISP membership. These instances were not reported to the Defence Security Incident Centre[81]; and
- in one instance, the project in question had ended. This instance was not reported to the Defence Security Incident Centre.[82]

4.11 Defence's review has identified that the risk of industry entities accessing highly security classified information and assets without DISP membership has been realised.

4.12 The ANAO reviewed the actions taken by Defence in response to these identified instances of non-compliance. The ANAO's review of Defence records indicates that as at 18 January 2021:

- none of the nine entities with active contracts had obtained DISP membership;
- five of the nine entities had not applied for DISP membership; and
- four of the nine entities had applied for DISP membership but Defence has not yet granted DISP membership to those entities.

4.13 In response to the ANAO's request for an update on the membership status of these nine entities, Defence informed the ANAO that as at June 2021:

- one of the nine entities was granted DISP membership on 22 April 2021;
- five of the nine entities had not applied for DISP membership; and
- three of the nine entities had applied for DISP membership but Defence had not yet granted DISP membership to those entities.

---

79 The membership records were held in Defence's DISMS (the system used by Defence prior to April 2019 to record DISP membership details). The 131 records represented all the DISP membership applications identified in DISMS as being 'in progress'. The review's primary goal was to finalise or deny the membership applications, as appropriate.

80 The DSPF defines a major security incident as any deliberate, negligent or reckless action that leads, or could lead, to the loss, damage, corruption or disclosure of official information or assets.

81 Defence was unable to explain to the ANAO why this was the case.

82 Defence was unable to explain to the ANAO why this was the case.

4.14 In these nine instances, Defence's response to industry entities operating without the appropriate levels of DISP membership was administrative and Defence had not adopted a risk-based compliance approach or pursued any of the actions available to it under the DSPF. Defence was unable to provide evidence that contract managers actively managed instances where it was drawn to their attention that DISP membership was not held.

4.15 As discussed in paragraphs 4.3 and 4.4, the DSPF states that non-compliance with DISP membership requirements may result in Defence downgrading, suspending or terminating an industry entity's membership. The DSPF also states that failure to comply with membership requirements may have other consequences, such as contractual, criminal or financial penalties. Defence records indicate that it has not taken any such actions in respect to the nine identified instances of non-compliance. In May 2021, Defence advised the ANAO that:

> Noting the broad range of contracts and the limited detail on particular projects available, Defence has not identified any application of contractual penalties for non-compliance with DISP membership requirements.

4.16 Further, there is no evidence that Defence has assessed the risks associated with the nine entities' historical or ongoing access to sensitive and security classified assets and information without appropriate levels of DISP membership. Information on AusTender indicates that Defence has continued to enter into contracts with some of these entities, despite them not having DISP membership.[83] Defence advised the ANAO in May 2021 that:

> DSPF Control 11.1 Project Security paragraph 17 requires a project to supply to DS&VS [Defence Security and Vetting Service] the Project Initiation Document (PID) and the Security Classification and Categorisation Guide (SCCG) (both DS&VS template documents). The PID has a check box to specify the highest level of classification required for the project - but does not currently provide any guidance on associated DISP requirements. Defence does not currently have additional guidance for projects to identify other contracts within the business area to consider security risks and implications relating to project security.
>
> Defence has identified the need for a more integrated approach to considering industry security risks and implications including aggregation across multiple projects/platforms/domains and is working to embed these considerations through improvements to controls and guidance.
>
> …
>
> Defence is undertaking a program of work through the Capability Acquisition Security Taskforce to identify entities and sectors requiring deeper consideration of security risks and mitigations.

Grant Hehir
Auditor-General

Canberra ACT
13 September 2021

83 It is not possible to determine from information on AusTender whether these contracts meet the DSPF definition for requiring DISP membership.

Appendices

Appendix 1 Department of Defence response

Australian Government
Department of Defence
PO Box 7900 CANBERRA BC ACT 2610

EC21-002905

Mr Grant Hehir
Auditor-General
PO BOX 707
CANBERRA ACT 2601

Dear Mr Hehir

Australian National Audit Office (ANAO) Section 19 Proposed Report – Defence's Contract Administration – Defence Industry Security Program.

Thank you for the opportunity to comment on the Proposed Report for the ANAO performance audit *Defence's Contract Administration – Defence Industry Security Program (DISP).* Defence acknowledges the findings and agrees to implement the proposed recommendations.

Defence has taken actions to enhance the effectiveness of the DISP and administration of Defence contracts, including through the implementation of the DISP *Assurance Program Lifecycle*. Through the DISP *Assurance Program Lifecycle*, Defence supports defence industry to improve security resilience and meet security obligations. More broadly, Defence is also working with defence industry to improve security policies, practices and outcomes.

Attached to this letter are Defence's Response to Requests for Information (**Annex A**), Defence's Response to the Proposed Recommendations (**Annex B**) and Defence's Summary Response (**Annex C**). These constitute Defence's formal response to the Section 19 Proposed Report.

Our point of contact is the ANAO Liaison Officer, Nicole Fry, who can be contacted by telephone on 02 6192 7974 or via email at: nicole.fry@defence.gov.au.

Yours sincerely

Greg Moriarty
Secretary

24 August 2021

Angus J Campbell, AO, DSC
General
Chief of the Defence Force

24 August 2021

Annexes:
A. Defence's Response to Requests for Information
B. Defence's Responses to Proposed Recommendations
C. Defence's Summary Response

Appendix 2 Performance improvements observed by the ANAO

1. The existence of independent external audit, and the accompanying potential for scrutiny improves performance. Improvements in administrative and management practices usually occur: in anticipation of ANAO audit activity; during an audit engagement; as interim findings are made; and/or after the audit has been completed and formal findings are communicated.

2. The Joint Committee of Public Accounts and Audit (JCPAA) has encouraged the ANAO to consider ways in which the ANAO could capture and describe some of these impacts. The ANAO's 2021–22 Corporate Plan states that the ANAO' s annual performance statements will provide a narrative that will consider, amongst other matters, analysis of key improvements made by entities during a performance audit process based on information included in tabled performance audit reports.

3. Performance audits involve close engagement between the ANAO and the audited entity as well as other stakeholders involved in the program or activity being audited. Throughout the audit engagement, the ANAO outlines to the entity the preliminary audit findings, conclusions and potential audit recommendations. This ensures that final recommendations are appropriately targeted and encourages entities to take early remedial action on any identified matters during the course of an audit. Remedial actions entities may take during the audit include:

- strengthening governance arrangements;
- introducing or revising policies, strategies, guidelines or administrative processes; and
- initiating reviews or investigations.

4. In this context, the below actions were observed by the ANAO during the course of the audit. It is not clear whether these actions and/or the timing of these actions were planned in response to proposed or actual audit activity. The ANAO has not sought to obtain assurance over the source of these actions or whether they have been appropriately implemented.

Improvements to Defence's contracting suites

5. The audit reviewed Defence's three main contracting suites to assess whether DISP requirements were clearly defined (see paragraphs 2.11 to 2.12). The ANAO found that there were opportunities for the templates to more clearly define contractual requirements, by:

- including a mandatory clause specifying if DISP membership is, or is not, required;
- requiring the contract drafter to specify the level of DISP membership the industry entity must hold for each of the four security elements of the DISP; and
- referencing current security policy.

6. Defence informed the ANAO that these findings have highlighted inconsistencies between various contracting templates, that it would review the use of DISP requirements across the contracting templates, and seek improvements through having a common DISP requirement clause across the various contracting suites.

Improvements to raising contract managers' awareness of the use of DISP membership clauses in contracts

7. The audit identified shortcomings in the application of DISP requirements in Defence's active contracts by its contract managers, and a need for clearer guidance to help Defence contract managers navigate the DISP throughout the procurement lifecycle (paragraphs 2.12 to 2.22).

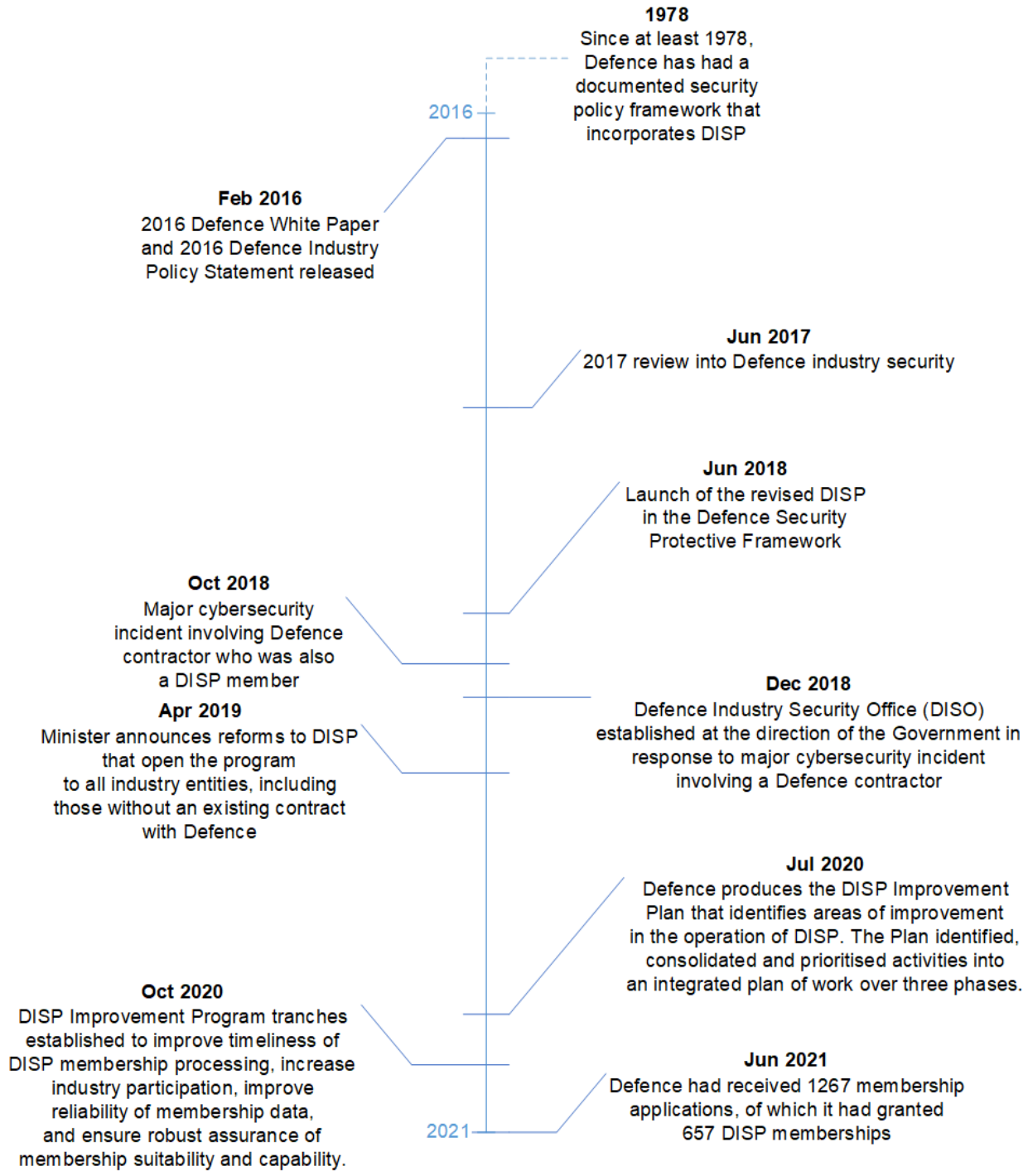
8. Defence informed the ANAO that it has made two improvements to address the shortcomings in contract managers' awareness of the use of DISP membership clauses in contracts.

- Defence is developing a web-based application to assist Defence contract managers through the procurement approval process, called 'My Procurements'. The aim of this application is to enable consistency of approach and compliance with processes and policies across Defence. Defence advised the ANAO that contract managers are now prompted to consider DISP requirements when using My Procurements to complete the procurement approval process. My Procurements is scheduled to be rolled out across Defence at the end of 2021.
- Defence plans to update the Defence Procurement Policy Manual[84] to include a new contracting requirement that Defence officials must consider DISP and the appropriate level of DISP membership in the procurement process.

84 The purpose of the Defence Procurement Policy Manual is to assist Defence officials to implement the requirements of the Commonwealth Procurement Rules (CPRs) and Defence policy when undertaking a procurement.

Appendix 3 Timeline of events

Figure A.1: Key dates in the history of the Defence Industry Security Program

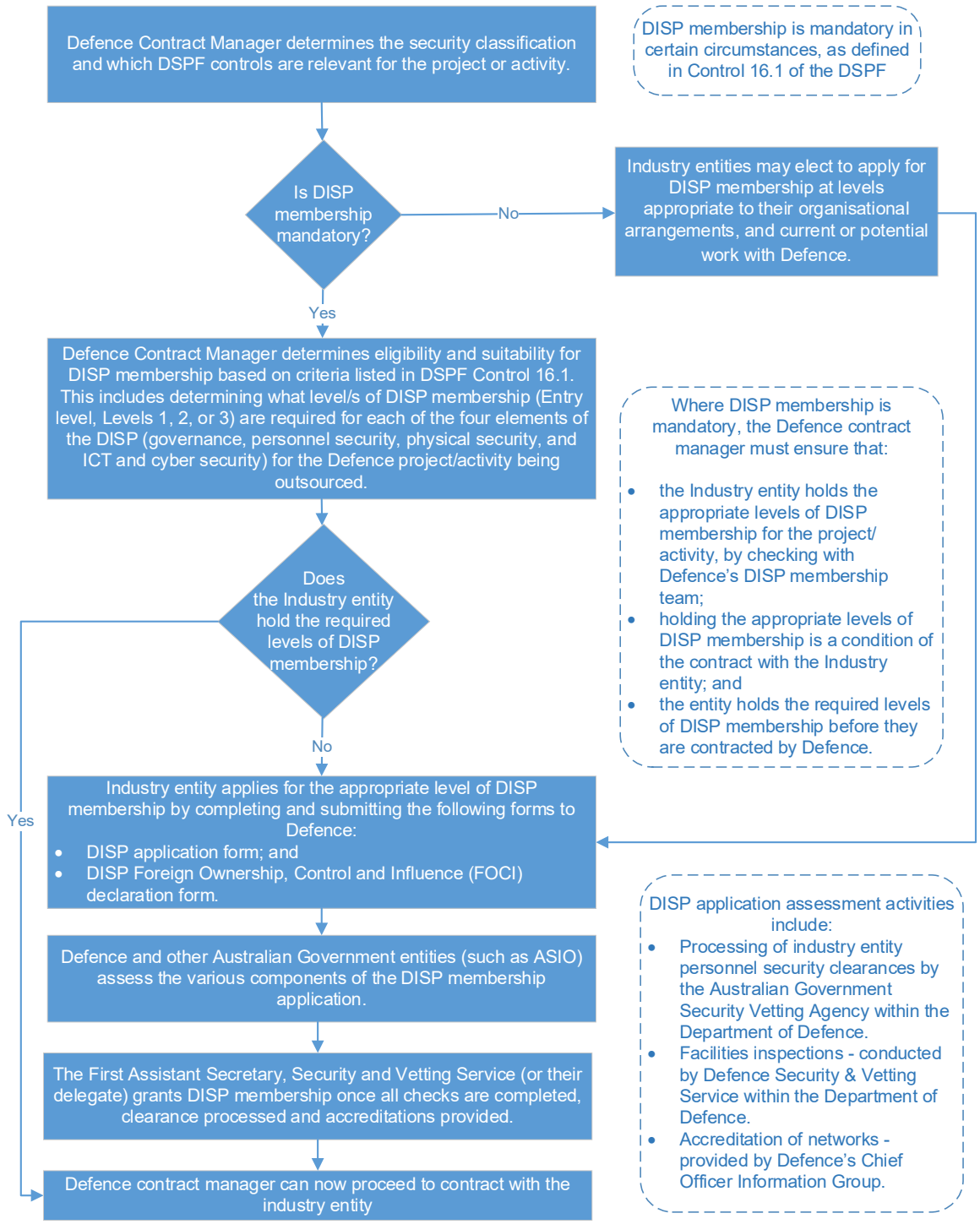


Source: Defence documentation.

Appendix 4 Summary of the DISP application process

1. The diagram below provides a simplified representation of the DISP application process as at March 2021.

Figure A.2: Summary of the DISP application process



Source: Defence documentation.

Appendix 5 2017 Review – Status of Recommendations

1. A 2017 review made recommendations to mitigate Defence industry security vulnerabilities and provide greater levels of assurance to government. On 20 June 2017, the Government agreed to all the recommendations from the review.

2. In October 2018, the Defence Security and Vetting Service provided a brief to the Defence Secretary and Chief of the Defence Force on the status of the updated Defence Industry Security Program. Table A.2 outlines the status of the recommendations reported in the 2018 brief and the ANAO's assessment of Defence's implementation of the six review recommendations relevant to this performance audit.

3. The approach used by the ANAO to assess the implementation status of the six selected recommendations is set out in Table A.1.

Table A.1: ANAO categorisation of implementation status

Assessment	
Not implemented	There is no supporting evidence that the agreed action has been undertaken, or the action taken does not address the intent of the recommendation as agreed.
Partially implemented	The action taken was less extensive than the recommendation agreed, as it: • fell well short of the intent of the recommendation as agreed; and/or • processes were initiated or implemented but outcomes not achieved.
Largely implemented	The action taken was less extensive than the recommendation as agreed, as it: • fell short of the intent of the recommendation as agreed, and/or • processes were initiated or implemented and there is evidence there was also action taken to achieve the outcome.
Implemented	There is supporting evidence that the agreed action has been undertaken, and the action met the intent of the recommendation as agreed.

Source: ANAO.

Table A.2: Status of Defence's implementation of six review recommendations relevant to the DISP

Review recommendation	Review findings which led to the recommendation	Defence's assessment of the status of the recommendation as of October 2018	ANAO assessment
Defence implement planned reforms to the DISP and enhance security assurance to assess DISP members' security performance and compliance with self-reporting obligations.	The data necessary to assess industry compliance with DISP self-reporting obligations was not consistently available or reliable.	In progress. The assurance framework will be implemented with the launch of the reformed DISP in early 2019.	**Not implemented.** As discussed in Chapter 3 of this audit, Defence has not established effective monitoring and assurance processes to assess compliance with contracted DISP requirements. In particular: • Defence does not have complete and accurate contract data to enable effective assessments of compliance with contracted DISP requirements. • Defence has designed an assurance framework to monitor compliance, but has only partially implemented this framework. • Defence has not undertaken a risk assessment of existing contracts to determine if there are contracts

Review recommendation	Review findings which led to the recommendation	Defence's assessment of the status of the recommendation as of October 2018	ANAO assessment
			with DISP clauses for which the contractor does not hold DISP membership, or DISP membership at the appropriate level.
The Defence Security Committee (DSC) regularly review defence industry security governance, performance against assurance targets and prioritisation of security assurance activities.	Defence's security assurance activities had not met policy intent, and security risk was not being considered consistently in the capability life cycle. Defence should monitor security assurance performance including the appropriate allocation and prioritisation of security assurance activities.	Complete.	**Partially implemented.** Defence informed the ANAO in June 2021 that assurance has been addressed through regular reporting to the Defence Security Committee. However, as discussed at paragraph 3.57 of this audit, the data is at a high level and not categorised by DISP membership.
Defence develop adequate metrics to support enterprise and operational management of security risk and policy implementation in its security reform initiatives.	Data to support an enterprise-level assessment of industry security risk such as the number and nature of DISP members and of DISP security incidents was either not available or not reliable. Constraints on information systems limits proactive management of the DISP and the development of industry security policy.	Complete.	**Partially implemented.** Defence advised the ANAO in June 2021 that enterprise-reporting on industry security is regularly provided to the Defence Security Committee. However, the constraints on information systems around DISP members and security incidents still remain (see Chapters 3 and 4 of this audit). Further, Defence has been unable to provide quarterly reporting to DSPF control owners on security incidents under their controls (see paragraph 3.60 of this audit), or monthly reporting to DISO on security incidents involving DISP members (see paragraph 3.56 of this audit).
Defence include security as a mandatory consideration in the smart buyer framework.	There was limited evidence that security risks were being routinely considered in capability project development or resourcing.	In progress. A security FIC [Fundamental Input to Capability] is being developed in consultation with CASG.[a]	**Implemented.**

Review recommendation	Review findings which led to the recommendation	Defence's assessment of the status of the recommendation as of October 2018	ANAO assessment
	Identification, treatment and resourcing of security risks was inconsistently managed through the capability life-cycle.		
Defence develop structured guidance on the security obligations of, and improve and deliver security threat advice to, Defence capability project and contract managers.	A number of Defence project and contract managers were unaware of their specific responsibilities for defence industry security assurance and were not accessing classified security advice.	In progress. The revised website will include tools and guidance for contract managers.	**Not implemented.** As discussed in Chapter 2 of this audit, Defence's tools and guidance for contract managers, and revised intranet site, were still being developed as of January 2021. Further, as discussed in Chapter 2 of this audit, Defence has not developed a single source of authoritative operational guidance to assist contract managers to accurately and consistently incorporate DISP requirements into contracts and monitor industry compliance with contractual obligations.
Defence implement DISP redesign and, in consultation with Chief Information Officer Group as appropriate, increase engagement with DISP members in the management of the DISP.	DISP engagement was too limited. Defence engagement with industry was described as 'inadequate and had declined in recent years'.	Defence did not report on this recommendation in the October 2018 brief. In June 2021, Defence advised the ANAO that it: 'combined recommendations 11 and 12 as they were addressed through the establishment of a new team with processes to address DISP management'.	**Partially implemented.** As discussed in Chapter 3 of this audit, Defence has sought to increase engagement with Defence industry members through the revised DISP external website, an online training course and roadshow events. Defence also has in place a helpdesk to provide support to stakeholders about the program and its requirements.

Note a: Defence defines Fundamental Inputs to Capability (FIC) as 'capability elements or inputs, which in combination, form the basis of capability. No individual FIC is a capability. Generating capability depends on integrating, coordinating and managing the various FIC, which need to be delivered in the quantities, characteristics and timescales to generate and sustain the capability, combined in an optimum way to deliver the joint force by design'. The nine FICs are: Organisation, Command and Management, Personnel, Collective Training, Major Systems, Facilities and Training Areas, Supplies, Support and Industry. Source: Defence Capability Manual, 22 December 2020, p. 12.

Source: ANAO analysis of Defence documentation.

Appendix 6 DISO required capabilities

1. In February 2021 the First Assistant Secretary, Defence Security and Vetting Service, advised the Associate Secretary that DISO is 'missing all or most of the capability' necessary for effective DISP information management and reporting'.

2. The capability requirements identified by Defence as requiring attention are summarised in Table A.3 below.

Table A.3: Defence Industry Security Office (DISO) required capabilities

DISO capability	Defence's assessment of capability	Overview of capability
DISO Management, DISP Policy, Service Improvement	Established capability	• Procurement and contract management. • Policy improvements. • Quality assurance of DISP process outcomes. • Project management and continuous improvement of processes.
DISP Admission	Developing capability	• Eliminate backlog. • Establish benchmarks at each membership level to achieve 750 applications per annum.[a] • Cyber assessment of all applicants and detailed independent risk assessment for DISP ICT security levels 1-3. • Certification and accreditation of facilities to support DISP physical security levels 1-3.
FOCI (Foreign Ownership, Control and Influence)	Developing capability	• Initial and ongoing assessment of applicant's actual or potential susceptibility to foreign influence. • Establish risk management and escalation processes. • Share information with procurement and capability managers. • Establish continuing assessment approach to reach 1,070 reassessments of 2,500 members per annum.
DISP Assurance	Missing all or most capability	• Establish risk-informed reassessment of 700 approved participants per annum to confirm ongoing suitability and capability. • Cyber reassessment and detailed independent risk assessment revalidation for DISP ICT security levels 1-3. • Reaccreditation of facilities to support DISP physical security levels 1-3. • Targeted, 'deep dive' audits of 15 participants per annum.
Outreach and Education	Missing all or most capability	• Targeted and tailored communication with industry to promote DISP participation and improve compliance with Defence's security needs. • Industry education for uplift, including cyber training. • Dedicated stakeholder communications, education and information for Defence about DISP.

DISO capability	Defence's assessment of capability	Overview of capability
Information Management, Analysis and Reporting	Missing all or most capability	• Establishment, maintenance and enhancement of DISP Customer Relationship Management (2,500 participants by June 2023). • Data analysis and reporting, to enable intelligence and risk–informed management of DISP members and effective targeting of assurance and audit activities.

Note a: The First Assistant Secretary, Defence Security and Vetting Services, advised the Associate Secretary in December 2020 that DISO would need to process an expected volume of 750 DISP membership applications a year (at a cost of approximately $10,000 per application) and the delivery of 'enhanced membership management'.

Source: Defence documentation.

Appendix 7 Compliance with DISP membership requirements for the four contracts reviewed by the ANAO

Table A.4: Compliance with DISP membership requirements as of August 2021 for four contracts reviewed by the ANAO

Contractor and details of contract	DISP clause in contract	Current DISP membership (after 1 April 2019)	ANAO comment
Luerssen Australia Pty Ltd (Luerssen). Offshore Patrol Vessels Acquisition Contract, signed 31 January 2018.	**Yes.** DISP membership is required under the details schedule of the contract.	**Yes, a DISP member since 30 June 2021.** Defence records indicate that Luerssen applied for DISP membership on 23 November 2020 and was granted DISP membership on 30 June 2021.	Although DISP membership was required under the OPV contract signed in January 2018, Defence records indicate that Luerssen was only granted DISP membership in June 2021.
Rheinmetall Defence Australia Pty Ltd (Rheinmetall) Land 400 Phase 2 Combat Reconnaissance Vehicles Acquisition Contract, signed 9 August 2018.	**Yes.** The Conditions of Contract state that 'The Contractor shall obtain and maintain membership of the Defence Industry Security Program (DISP) in accordance with DSM Part 2:42.'	**Yes. A DISP member since 15 August 2018.** Defence records indicate that Rheinmetall applied for DISP membership (as required for existing members) on 28 May 2019 and was granted an updated DISP membership on 16 January 2020.	Defence records indicate that Rheinmetall has had updated DISP membership since January 2020. Defence records indicate that Rheinmetall also previously held DISP membership in August 2018 when the contract was signed.
Naval Group Australia (Naval Group). Submarine Design Contract, signed 1 March 2019.	**Yes.** DISP membership is required under the details schedule of the contract.	**Yes. A DISP member since contract signature.** Defence records indicate that Naval Group applied for DISP membership on 28 November 2019 and was granted DISP membership on 23 September 2020. Defence records indicate that Naval Group was previously granted DISP membership in August 2015.	Defence records indicate that Naval Group has DISP membership as required under the Submarine Design Contract.

Contractor and details of contract	DISP clause in contract	Current DISP membership (after 1 April 2019)	ANAO comment
Austal Ships Pty Ltd (Austal) Evolved Cape Class Patrol Boat Acquisition Contract, signed 30 April 2020.	**Yes.** DISP membership is required under the details schedule of the contract. The details schedule specifies that Austal requires FOR OFFICIAL USE ONLY level DISP membership for each security element.	**Not a DISP member.** Defence records indicate that Austal applied for DISP membership on 24 March 2021. As at 8 June 2021, Austal's application was still being processed.	Defence records indicate that Austal does not currently have DISP membership. Defence records indicate that Austal was previously granted DISP membership in August 2001. Defence advised the ANAO that all memberships granted prior to April 2019 were no longer recognised by Defence after 9 April 2021.

Source: ANAO analysis of Defence documentation.