The Auditor-General
Auditor-General Report No.50 2024–25
Performance Audit

Department of Defence’s Sustainment of Canberra Class Amphibious Assault Ships (Landing Helicopter Dock)

Department of Defence

Australian National Audit Office

Audit snapshot

Auditor-General Report No.50 2024–25

Department of Defence's Sustainment of Canberra Class Amphibious Assault Ships (Landing Helicopter Dock)

Why did we do this audit?

- The Royal Australian Navy's (Navy) amphibious warfare fleet includes two Canberra class amphibious assault ships, known as landing helicopter docks (LHDs).
- Since entry of the LHDs into service in 2014, Defence has contracted its core LHD sustainment delivery activities to industry.
- This audit provides assurance to Parliament on the effectiveness of Defence's sustainment arrangements for the LHD capability.

Key facts

- Arrangements for the sustainment of the LHDs have changed over time across three contractual phases or models: transition to sustainment; asset class prime contractor; and the Maritime Sustainment Model.
- LHD sustainment has the fourth highest expenditure across all sustainment products in the maritime domain, with funding of $180 million in 2024–25.

What did we find?

- Defence's arrangements for the sustainment of Navy's LHDs have been partly effective.
- Defence did not plan effectively for the transition from acquisition to sustainment. Value for money was not clearly demonstrated and probity was not well managed in the three relevant procurement activities.
- Defence has not managed its LHD sustainment contracts effectively. The LHDs have operated with ongoing deficiencies and have experienced critical failures during operations.
- Monitoring and reporting in respect to LHD sustainment outcomes, the extent to which Navy's requirements have been met, and the implementation of the Maritime Sustainment Model arrangements has been partly effective.

What did we recommend?

- There were nine recommendations to the Department of Defence aimed at improving: the transition from acquisition to sustainment; effective management of sustainment; and contract management, including potential fraud concerns.
- Defence agreed to the recommendations.

$1.9 bn
estimated cost of LHD sustainment for the decade to 2033–34

30 years
remaining on the LHDs' planned life-of-type, with withdrawal planned for 2055 and 2056

223
open urgent defects reported for the LHDs in June 2025

Summary and recommendations

Background

1. The Royal Australian Navy (Navy) amphibious warfare fleet includes two Canberra class amphibious assault ships, also known as landing helicopter docks (LHDs). These are HMAS *Canberra*, commissioned in November 2014, and HMAS *Adelaide*, commissioned in December 2015. The role of the LHDs is to provide capabilities in amphibious warfare, humanitarian assistance, disaster relief and sealift, and to contribute to broader naval activities. Effective sustainment of the LHDs, including maintenance and support, is essential for the effective delivery of these capabilities.

2. Defence's Naval Shipbuilding and Sustainment Group has been responsible for the sustainment of the LHDs on behalf of the Navy (the capability manager) since October 2022.[1] Since entry into service in 2014, Defence has contracted its core LHD sustainment delivery activities to industry. Defence's contracting model has changed from time to time, with each of the arrangements established at the commencement of the following three phases: the transition from acquisition to sustainment (from 2014 to 2019); the asset class prime contractor model (from 2019 to 2024); and the Maritime Sustainment Model (as of 1 July 2024).

Rationale for undertaking the audit

3. In 2024–25, Defence's sustainment activities for its fleet of two Canberra class amphibious assault ships, or LHDs, had a funding provision of $180 million (estimated at $1.9 billion to 2033–34). With service life-of-type until the mid-2050s, the LHDs provide Navy with amphibious capabilities which are to support the delivery of the Australian Government's strategic intent through joint Australian Defence Force (ADF) deployments. This audit provides assurance to the Parliament on Defence's sustainment of naval capability, building on Auditor-General Report No.30 2018–19 *ANZAC Class Frigates — Sustainment*.

Audit objective and criteria

4. The audit objective was to examine the effectiveness of Defence's sustainment arrangements for Navy's Canberra class fleet of amphibious assault ships (or LHDs).

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

- Has Defence implemented fit-for-purpose planning and value for money procurement arrangements to support its sustainment activities?
- Has Defence effectively managed its sustainment contracts?
- Has Defence established appropriate performance monitoring and reporting arrangements?

1 Prior to October 2022, the acquisition and sustainment of the LHDs was managed by the Capability Acquisition and Sustainment Group (CASG). CASG assumed this role from the former Defence Materiel Organisation (DMO) on 1 July 2015 when the DMO was delisted, and those functions were transferred to the Department of Defence. References to Defence in this report include the Department of Defence and the DMO prior to 1 July 2015.

Conclusion

6. Defence's sustainment arrangements for Navy's LHDs have been partly effective. Risks arising from an accumulation of defects and maintenance backlogs over several years have materialised. The substandard condition of the vessels, and personnel workforce shortages, have resulted in instances of critical failure and impacts to the Navy's delivery of operational outcomes.

7. Defence did not implement fit-for-purpose planning and value for money procurement arrangements to support LHD sustainment. Defence's future sustainment requirements, including access to important intellectual property for the LHDs, were not sufficiently developed during the acquisition phase. Establishment of the sustainment arrangements was delayed, occurring during the transition to sustainment process and alongside remediation activities to address issues persisting from acquisition. Defence's remediation activities did not achieve the required outcomes, resulting in additional work being transferred to the sustainment phase or managed as part of capability improvement projects.

8. Value for money and the intended sustainment outcomes were not achieved through Defence's procurement processes. Early cost estimates for the sustainment of the LHDs were under developed and did not anticipate the impact of the protracted acquisition deficiencies extending into sustainment and continuing into 2025. Defence has regularly reviewed and adjusted its sustainment budget.

9. Sustainment of the LHDs was not managed effectively by Defence through its prime contractor arrangements. Governance arrangements, contract management guidance, and risk management practices were not implemented in a timely manner and contract-specific probity arrangements were not developed. Defence did not take reasonable steps, as required by the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), to manage systemic poor procurement practices by the prime contractor or investigate claims of fraudulent activity in sub-contracting arrangements in accordance with its own policies. Defence did not use the full range of contractual levers available to manage its primary sustainment contract. This approach impacted the quality of service delivery and undermined the achievement of value for money through the contract.

10. Defence has established partly appropriate performance monitoring and reporting arrangements for the Canberra class LHDs. Sustainment outcomes have largely met Navy's requirements for the operational use of the platforms. The long-term availability and reliability of the LHDs is at risk primarily due to the accumulation of urgent defects, maintenance backlogs and shortfalls in personnel to undertake organic level maintenance. As a result, the LHDs have experienced critical failures, impacting on Navy operations.

11. Defence's transition to the new Maritime Sustainment Model lacked reliable and complete information on the expected performance of sustainment contractors. Value for money outcomes for the procurements under the new model were limited by poorly implemented probity arrangements and the procurements commencing later than planned, reducing the time available to resolve issues during contract negotiations.

Supporting findings

Planning and procurement

12. Defence accepted delivery of the ships from BAE in 2014 and 2015 later than planned and with defects and deficiencies in both vessels, many of which remain unresolved.

- In 2017, Defence established a Transition and Remediation Program (TARP) to manage the transition into sustainment and conduct the remediation work required to achieve the full capability expected from the LHDs. The remediation activities did not achieve all the intended outcomes, and in November 2019, Defence accepted the LHDs into full service with six 'significant residual deficiencies'.
- In 2021, Defence established a capability assurance program to address urgent operational and safety issues for the LHDs, including issues carried over from the TARP.
- In July 2024, one quarter of the way through the planned life of the ships, Defence closed the acquisition project with significant defects and deficiencies from acquisition remaining unresolved and to be managed during the sustainment phase (see paragraphs 2.2 to 2.21).

13. The integrity of Defence's procurement processes for the LHD sustainment prime contractors was undermined by poor controls over probity risks.

- In 2014, the Capability Support Coordinator contract was awarded following an open tender process. The effectiveness of this procurement was limited by issues in the planning and evaluation processes. There were also shortcomings in the subsequent extension of the services with the incumbent provider under the Major Service Provider Panel following an unsolicited proposal in 2022.
- In 2014, the Transition In-Service Support Contract was awarded following a 'collaborative' sole source procurement process involving protracted engagement by Defence to improve an under-developed tender response. The procurement outcome did not demonstrate value for money.
- In 2018, the Asset Class Prime Contractor was awarded following a two-stage selection process which involved assessments against fit-for-purpose evaluation criteria. The integrity of the process was compromised by the departure of a senior Defence official with early involvement in the procurement who was then employed by, and negotiated with Defence on behalf of, the winning tenderer (see paragraphs 2.22 to 2.77).

14. Defence's forecast and management of sustainment costs have been impacted by deficiencies from acquisition extending into sustainment. Since final operating capability was declared in 2019, the LHD sustainment funding provision per financial year has not met in-year requirements, with some sustainment work deferred and future costs increasing. In 2024 senior Defence officials considered options to address Navy sustainment funding pressures. Following consultation with the Minister for Defence in 2024, Navy sustainment funding was increased by an additional $300 million over two years to June 2026, of which Defence allocated $36 million towards LHD sustainment funding for 2024–25 (see paragraphs 2.78 to 2.88).

Sustainment management

15. Defence established governance arrangements to support its management of LHD sustainment contracts. These arrangements were either not implemented effectively or not maintained by Defence, resulting in a number of shortcomings.

- Since 2012, updates to the Materiel Sustainment Agreement (head agreement) between Navy and the Naval Shipbuilding and Sustainment Group have not been timely, occurring several years after key changes in responsibilities or organisational restructures had taken effect.
- A contract management plan was not established for the first 17 months of the ACPC contract. Contract risks, including those identified during the procurement process, were not revisited as planned or covered in the contract management plan.
- Contract-specific probity arrangements were not established for the ACPC contract. Defence relied solely on its broader departmental arrangements instead, which require Defence personnel to proactively identify and declare any actual, potential or perceived conflicts of interest as and when they arise.
- LHD sustainment risks at the strategic level are managed separately and in isolation from risks at the operational and technical levels. There is no hierarchy or clear line of sight between the risks identified in the Materiel Sustainment Agreement and those being managed day-to-day (see paragraphs 3.2 to 3.32).

16. Defence did not manage its primary LHD sustainment contracts as intended by its performance-based design. As a result, Defence cannot assure itself or ministers that sustainment services were delivered effectively and in accordance with the contracted requirements. Key deficiencies were that Defence did not:

- ensure that all mandatory reports were submitted in a timely manner by the contractor;
- undertake full or timely assessments of the contractor's performance;
- ensure that all key sustainment deliverables had been completed in full prior to making payments to the contractor; or
- use the full range of levers available in the contract to drive satisfactory performance.

17. Between 2021 and 2023 there were at least three separate allegations of fraudulent activities or instances of poor sub-contracting practices related to the ACPC contract. Defence did not seek further information from the contractor on the 2023 allegations and did not change its approach to managing the contract after being notified of the various issues (see paragraphs 3.33 to 3.79).

Performance monitoring and reporting

18. Defence has established a sustainment performance framework for the LHDs, with performance measures set out in a written agreement and reporting provided to senior Defence leadership. The performance measures adopted are relevant to the LHDs but are not fully reliable and do not provide a complete and clear picture of sustainment performance as some important areas of sustainment are not covered. For some performance measures, the nature of the targets selected has led to reporting that does not provide a fair presentation of performance results for the LHDs (see paragraphs 4.2 to 4.18).

19. Navy's operational requirements have been impacted by shortcomings in the management of LHD sustainment. Sustainment outcomes have included an accumulation of urgent defects, persistent maintenance backlogs, and the degradation of the condition of the platforms. The LHDs have fallen short of meeting availability targets since 2020–21 and sustainment-related deficiencies and workforce shortfalls have given rise to risks involving critical failures in the vessels, possible damage to Navy's reputation and concerns for the sustainability of the LHDs over the long-term. Some of these risks have materialised, including:

- total power failures in 2022 and 2023, making the LHDs temporarily unavailable while providing humanitarian assistance and disaster relief support in Tonga and Vanuatu; and
- a reduction from three ships to two available for deployment in the amphibious force during 2025 (see paragraphs 4.19 to 4.53).

20. In July 2024, Defence transitioned LHD sustainment to the 'Maritime Sustainment Model', which involved the procurement and contracting of new commercial arrangements. Defence started the procurements later than planned, which limited the options available to Defence to manage issues and strengthen value for money outcomes during negotiations. Arrangements to manage probity were not robust and, in respect to the LHD Capability Life Cycle Manager procurement, probity was poorly managed. Defence has not benchmarked or established expected sustainment performance levels for the Maritime Sustainment Model (see paragraphs 4.54 to 4.83).

Recommendations

Recommendation no. 1
Paragraph 2.18

The Department of Defence ensures that appropriate arrangements are in place for its transition and remediation programs to improve the rigour with which these activities are managed, and provide assurance that the relevant objectives have been achieved.

Department of Defence response: *Agreed.*

Recommendation no. 2
Paragraph 2.87

To support the future requirements for the LHDs, the Department of Defence develops and maintains class-specific life cycle sustainment plans for the Navy fleet, including funding requirements for the planned life of type, to ensure that the required capability is maintained across the classes' whole of life, at a rate of agreed availability.

Department of Defence response: *Agreed.*

Recommendation no. 3
Paragraph 3.6

The Department of Defence promptly reviews and updates, Navy's Materiel Sustainment Agreements with the Capability Acquisition and Sustainment Group and Naval Shipbuilding and Sustainment Group, following significant changes in organisational structures, or at least every three years.

Department of Defence response: *Agreed.*

Recommendation no. 4 **Paragraph 3.31**	The Department of Defence reviews and documents its LHD risk management arrangements, including the use of various ICT systems and oversight forums, with a view to identifying efficiencies, where possible, and ensuring that risks are appropriately identified, and actively managed with clear line of sight. **Department of Defence response:** *Agreed.*
Recommendation no. 5 **Paragraph 3.69**	Where the Department of Defence is notified of incidents such as suspected fraud or unethical conduct, the Department of Defence ensures that its response is fully documented and conforms to Defence policies and the *Commonwealth Fraud and Corruption Control Framework*. **Department of Defence response:** *Agreed.*
Recommendation no. 6 **Paragraph 3.78**	Where the Department of Defence's contracts with industry include mechanisms to obtain assurance over the completion of activities under the contract and the performance of suppliers, the Department of Defence ensures that contractual mechanisms are implemented. **Department of Defence response:** *Agreed.*
Recommendation no. 7 **Paragraph 4.13**	The Department of Defence review the performance measures for the sustainment of the LHDs to support a more reliable and complete assessment of sustainment performance. **Department of Defence response:** *Agreed.*
Recommendation no. 8 **Paragraph 4.63**	The Department of Defence establishes arrangements to ensure that its internal policies for the establishment of appropriate probity processes commensurate with the size, scale and risk of its procurement activities are complied with. **Department of Defence response:** *Agreed.*
Recommendation no. 9 **Paragraph 4.82**	The Department of Defence benchmarks and monitors sustainment performance under the Maritime Sustainment Model to enable an assessment of the achievement of its strategic objectives. **Department of Defence response:** *Agreed.*

Summary of entity response

21. The proposed audit report was provided to the Department of Defence. Extracts of the proposed audit report were provided to BAE Systems Australia Pty Ltd, Babcock Pty Ltd, and Kellogg Brown and Root Pty Ltd. The Defence summary response is provided below and its full

response is provided at Appendix 1. Responses from BAE Systems Australia Pty Ltd, Babcock Pty Ltd, and Kellogg Brown and Root Pty Ltd are provided at Appendix 1.

> The Department of Defence acknowledges the findings contained in the Auditor General's report on the sustainment of the Canberra Class amphibious assault ships.
>
> Defence acknowledges that planning and procurement processes, sustainment management arrangements and performance monitoring and reporting were assessed as partly effective.
>
> Defence supports the recommendations. Defence is committed to ensuring the through-life sustainment of the Canberra Class amphibious assault ships deliver the best possible capability outcomes for the Australian Government and the Australian Public.

Key messages from this audit for all Australian Government entities

22. 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.

Policy and program design

To appropriately manage assets throughout the asset life cycle, entities should prepare long-term plans that consider whole-of-life costs and strategies and that are updated to reflect changes in the operating environment and then act in accordance with the plans.

The Auditor-General
Auditor-General Report No.31 2024–25
Performance Audit

Maximising Australian Industry Participation through Defence Contracting

Department of Defence

Australian National Audit Office

Audit snapshot

Auditor-General Report No.31 2024–25

Maximising Australian Industry Participation through Defence Contracting

Why did we do this audit?

- The Department of Defence (Defence) is required to maximise Australian industry participation through contracted plans and schedules with its suppliers. Since 2019, these requirements have been primarily conveyed through the *Defence Policy for Industry Participation* (DPIP).
- This audit was conducted to provide assurance to the Parliament on the effectiveness of Defence's approach to maximising Australian industry participation through its contracting activities.

Key facts

- Materiel and non-materiel procurements valued at or above $4 million are to include Australian industry schedules or plans.
- Construction services procurements valued at or above $7.5 million are to include Local Industry Capability Plans.

What did we find?

- Defence has not maximised Australian industry participation through the administration of its contracts.
- Defence's administrative arrangements for maximising Australian industry participation through its procurement and contracting activities are partly fit for purpose.
- Defence did not effectively implement relevant industry contracting requirements with respect to the eight executed contracts examined.
- Defence has established partly appropriate governance, assurance and reporting arrangements to oversee the implementation of its contracting requirements.

What did we recommend?

- There were 9 recommendations to Defence aimed at improving governance, assurance and reporting arrangements.
- Defence agreed to all 9 recommendations.

$38.7 bn

Total value of Defence procurements in 2022–23.

$10.6 bn

Australian Bureau of Statistics estimation of the Australian defence industry's contribution to the broader Australian economy 2022–23.

79%

Percentage of Defence spending that occurs in Australia.

Summary and recommendations

Background

1. For the financial year 2022–23, the Department of Defence (Defence) ranked as the Australian Government's largest procurer with 51.7 per cent of Commonwealth entity contracting, valued at $38.69 billion.[1] Successive Australian governments have encouraged the involvement of domestic industries in Defence procurement to develop and maintain the industrial base, secure supply chains, and promote employment and economic growth.

2. Defence initiatives to maximise the opportunities for domestic suppliers to participate in government procurement include the Australian Industry Capability (AIC) Program, launched in February 2008.[2] The AIC Program required potential contractors to demonstrate how their tenders provide opportunities for Australian businesses.

3. On 28 March 2019, the Minister for Defence Industry released the *Defence Policy for Industry Participation* (DPIP) to improve consistency in Defence's approach to maximising Australian industry's opportunity to participate in Defence procurement. The DPIP requires Defence to consider AIC plans or schedules (or Local Industry Capability plans for construction projects) during procurement decision-making and to ensure the industry commitments in those plans are captured as contracted obligations in materiel and non-materiel procurements valued at or above $4 million, and construction procurements at or above $7.5 million.

Rationale for undertaking the audit

4. Defence's implementation and delivery of contracted Australian industry requirements has been an area of focus for successive governments and an ongoing interest for the Parliament. The government intent to maximise Australian industry involvement in Defence procurement was reflected in the AIC Program in 2008 and reaffirmed in the 2016 *Defence Industry Policy Statement* and the 2018 *Defence Industrial Capability Plan*. This audit provides the Parliament with independent assurance on the effectiveness of Defence's arrangements to deliver Australian industry policy outcomes through its contractual arrangements with its suppliers.

Audit objective and criteria

5. The objective of the audit was to examine the effectiveness of Defence's administration of contractual obligations to maximise Australian industry participation.

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

- Have fit-for-purpose administrative arrangements been established to maximise Australian industry participation in Defence procurement and contracting?

1 Department of Finance, *Statistics on Australian Government Procurement Contracts*, available from https://www.finance.gov.au/government/procurement/statistics-australian-government-procurement-contracts- [accessed 11 April 2025].

2 The AIC Program, incorporating requirements for AIC plans, was foreshadowed in the *Defence and Industry Policy Statement 2007.* In February 2008, the AIC program was launched by the Parliamentary Secretary for Defence Procurement.

- Have applicable contracting requirements been implemented to maximise Australian industry participation?
- Has Defence implemented appropriate governance, assurance and reporting arrangements to support the objective of maximising Australian industry participation?

Conclusion

7. Defence has not maximised Australian industry participation through the administration of its contracts. Defence industry policy and contracting requirements were not applied to all relevant procurements, and — where supplier commitments have been contracted — Defence has not effectively monitored or ensured the delivery of those obligations.

8. Defence's administrative arrangements for maximising Australian industry participation through its procurement and contracting activities are partly fit for purpose. Defence's procurement framework has not been updated in a timely manner, and as at August 2024, did not fully reflect the requirements of the March 2019 DPIP. Guidance for Defence personnel in relevant tendering and contracting templates is incomplete, and in some cases outdated. Defence engages with industry through forums and other activities as well as through individual procurement processes to support the intent of government's industry contracting policy.

9. Defence has not implemented applicable contracting requirements effectively. Of the eight contracts examined, each had one or more important shortcomings resulting from limitations in Defence's advice to potential suppliers, weaknesses in Defence's contracting of industry participation commitments, and ineffective monitoring of supplier compliance with those commitments.

10. Defence's governance, assurance and reporting arrangements for industry participation are partly appropriate. Senior Defence committees have received reports on activities to support Australian industry policy objectives. Defence did not establish the Industry Policy Division working group to periodically review the policy in accordance with the DPIP. The AIC Plan assurance framework does not align with a professional standard-setting framework and activities conducted under that framework do not provide reasonable assurance over the matters examined. Defence reports on Australian industry expenditure and has undertaken to further develop its reporting as part of the 2024 *Defence Industry Development Strategy*.

11. As outlined in the 2024 *Defence Industry Development Strategy*, Defence was to update the DPIP in late 2024. This policy update follows the 2023 *Defence Strategic Review* and the 2024 *National Defence Strategy*. Effective implementation of the next iteration of Australian defence industry contracting policy will require appropriate administrative and IT support systems, including sound procurement controls and contract management activities.

Supporting findings

Administrative arrangements

12. Defence gives effect to its Australian industry contracting requirements through its internal policy framework. Defence's framework is informed by requirements under the *Public Governance, Performance and Accountability Act 2013*, the Commonwealth Procurement Rules and government's Defence industry policies, as set out by the *2016 Defence Industry Policy*

Statement and the *2018 Defence Industrial Capability Plan*. Key elements of Defence's established policy framework, such as the Defence Procurement Manual (DPM) and its contracting templates, were not updated in a timely manner following the release of the DPIP in March 2019. The DPM was not updated until 1 July 2020, 15 months after the DPIP's release. Defence lacks arrangements to ensure that procurement documents and contracting templates are aligned with the DPIP requirements, and up to date. Automated system controls, which were established in 2022 and mandated in 2024 — to improve compliance with mandatory procurement policies — do not cover the requirements of the DPIP. (See paragraphs 2.2 to 2.41)

13. Guidance on the Australian Standard for Defence Contracting (ASDEFCON) and the Suite of Facilities tendering and contracting templates is incomplete, with additional guidance notes planned but not developed and released. Defence does not assess its personnel training data by role and therefore cannot provide assurance that its procurement and contracting staff have undertaken training relevant to their roles. The dedicated AIC training course announced in February 2019 is primarily focused on materiel procurements and was not implemented until September 2022. (See paragraphs 2.42 to 2.67)

14. Defence has undertaken a range of industry engagement activities to support the objective of maximising Australian industry participation in procurement. These activities have included the establishment of an Australian Industry Capability Forum and engagements with industry associations. In the absence of a communications strategy for the DPIP, Defence is unable to measure the effectiveness of the information and guidance it has provided to industry on the industry contracting policy requirements in place since 2019. (See paragraphs 2.68 to 2.80)

Implementation of requirements

15. Defence's advice on Australian industry contracting requirements was provided to potential suppliers as part of the relevant tender processes. Each of the eight contracts examined contained one or more shortcomings with respect to this advice or in the contracting materials provided by Defence, including:

- Defence not considering industry contracting requirements during the early stage of the procurement and therefore not advising suppliers of all requirements;
- the rationale for exemptions from implementing Australian industry contracting requirements not being documented by Defence; and
- outdated or incorrect terminology and reference material being used by Defence or available to suppliers. (See paragraphs 3.6 to 3.15)

16. Of the eight contracts examined, the relevant suppliers for four had provided Defence with a project or industry plan (or schedule) in accordance with the procurement stage requirements of the DPIP. By 29 August 2024, one of these plans (or schedules) remained in draft and had not been further developed as required, and three had been finalised and approved by Defence. For the five contracts without finalised plans, Defence did not document the exemption from this requirement for three suppliers, provided one supplier with an extension to 20 June 2023, and did not finalise the draft plan for the remaining supplier.

17. For four examined contracts, additional AIC or LIC commitments were also within other contract documents. For the two examined contracts with no plans or schedules developed, AIC or LIC commitments were located in other contract artefacts such as a service management plan

or statement of work. Unclear or imprecise clauses were included in the contract documentation for three contracts. Of the five that met the threshold for the publication of an AIC Plan, one was published on Defence's website. Shortfalls in record keeping were observed in the documentation for each of the eight contracts. (See paragraph 3.16 to 3.33)

18. Defence undertakes limited monitoring to ensure the delivery of contracted Australian industry commitments. Where suppliers have reported against their DPIP-related commitments, this reporting has not been complete, with 12 of 59 relevant measures reported against. For four of the five contracts where supplier commitments have been contracted:

- the reporting to Defence indicated that these commitments were not being delivered. Defence undertook follow up action with respect to one of those contracts; and
- the DPIP-related terms in Defence's contract with the head contractor are required to 'flow down' as requirements to the head contractor's subcontractors. One of these four suppliers has reported to Defence on its engagement with subcontractors. (See paragraphs 3.34 to 3.46)

Governance, assurance and reporting

19. Senior Defence committees at the enterprise and group levels have received reports on the implementation of activities relevant to the DPIP, including the implementation of the 'enhanced' Australian industry capability (AIC) contractual framework announced in mid-2020. The policy oversight forum responsible for the periodic review and alignment of the policy with government's defence industry policy objectives was not established as foreshadowed by the DPIP. In the absence of this forum, Defence has not regularly reported on the DPIP or monitored its implementation activities to ensure a unified approach at a whole-of-enterprise level, consistent with the intent of the DPIP. (See paragraphs 4.2 to 4.15)

20. Defence's assurance framework does not prescribe the level of assurance to be obtained and does not align with an auditing standards framework. Defence's 'AIC Audit Program' has provided limited insights on the extent to which Defence is implementing its DPIP obligations or whether suppliers are meeting their contracted DPIP-related commitments. Assurance activities conducted under Defence's framework are limited to materiel contracts over $20 million in value, representing one-fifth of the procurement categories covered by the DPIP. The scope of Defence's assurance program has included contracts that were executed prior to the March 2019 introduction of the DPIP. Of the 17 assurance activities conducted by Defence since July 2021, seven did not report the deficiencies identified in AIC plans as non-compliance, as the DPIP did not apply to those contracts.

21. Other assurance-related activities such as Defence's self-reporting through compliance surveys under its Supplier Rating System indicate that Defence has not fully complied with its obligation to ensure supplier commitments are contracted in accordance with the DPIP. Of the 768 contract surveys conducted as at July 2024, 209 (27 per cent) reported that AIC obligations were 'not applicable'. Other procurement and contracting compliance arrangements in Defence do not cover the DPIP's requirements and have therefore not identified issues relating to its implementation. (See paragraphs 4.16 to 4.38)

22. Defence has established performance measures related to its engagement with Australian industry and provides quarterly reporting to the Minister for Defence. Defence's administrative

systems do not support reporting at the project level or ensure that AIC Plans are published where required. Defence has undertaken to further develop its reporting on defence industry as part of its implementation of the Defence Industry Development Strategy. (See paragraphs 4.39 to 4.57)

Recommendations

Recommendation no. 1
Paragraph 2.32

The Department of Defence establish arrangements to ensure that its contract template and guidance documents are up to date and aligned with Defence industry contracting and policy requirements.

Department of Defence response: *Agreed.*

Recommendation no. 2
Paragraph 2.40

The Department of Defence implement controls within relevant systems for its procurement, financial, and contract management activities to support and monitor compliance with its obligations to implement Australian industry participation and contracting requirements.

Department of Defence response: *Agreed.*

Recommendation no. 3
Paragraph 2.60

The Department of Defence complement the implementation of its new procurement and contract management training by:

(a) establishing measures to inform senior leadership of the extent to which role specific training is completed, such as by procurement and contract managers; and

(b) incorporating requirements for Defence policies, such as the DPIP, into mandatory training.

Department of Defence response: *Agreed.*

Recommendation no. 4
Paragraph 2.64

The Department of Defence extend the scope of the existing AIC Practitioners course to cover the needs of users of Defence contracting material beyond the ASDEFCON suite.

Department of Defence response: *Agreed.*

Recommendation no. 5
Paragraph 3.32

The Department of Defence implement measures to ensure that:

(a) where approval of industry commitments occurs after contract execution, this takes place within agreed timeframes and includes options for remediation and contract termination if this does not take place; and

(b) public AIC plans are prepared and published where required.

Department of Defence response: *Agreed.*

Recommendation no. 6
Paragraph 3.40

The Department of Defence improve its administrative arrangements for contracts to ensure that:

(a) contracts with industry participation-related requirements can be efficiently and effectively identified and managed; and

(b) contracted industry participation-related measures can be efficiently and effectively identified and monitored.

Department of Defence response: *Agreed.*

Recommendation no. 7
Paragraph 3.45

The Department of Defence:

(a) monitor subcontractor performance of industry participation commitments where there are contractual flow down requirements between head contractors and their subcontractors; and

(b) incorporate details on the potential for flow down industry participation requirements into relevant guidance for Defence personnel and industry.

Department of Defence response: *Agreed.*

Recommendation no. 8
Paragraph 4.14

The Department of Defence improve its oversight arrangements to monitor and drive appropriate consistency in its implementation of Australian industry policy in its procurement and contracting activities.

Department of Defence response: *Agreed.*

Recommendation no. 9
Paragraph 4.37

The Department of Defence review and revise its AIC assurance framework to:

(a) prescribe the level of assurance to be obtained through the assurance activities;

(b) cover the full scope of Defence industry contracting and policy requirements; and

(c) assess whether Defence industry contracting and policy requirements have been considered and addressed early in procurement processes as required, including the approval and documentation of exemptions.

Department of Defence response: *Agreed.*

Summary of entity response

23. The proposed audit report was provided to the Department of Defence. Defence's summary response is provided below, and its full response is included at Appendix 1. Improvements observed by the ANAO during the course of this audit are listed in Appendix 2.

Defence acknowledges the findings of the Auditor-General's Performance Audit report: *Maximising Australian industry participation through Defence contracting*. Defence is committed to ensuring that Australian industry participation in Defence contracts is considered and optimised in the delivery of Defence capabilities.

Defence accepts the key findings and recommendations aimed at enhancing governance, assurance, reporting arrangements, relevant training and guidance when implementing Australian industry participation policy requirements in Defence procurements.

In alignment with the Defence Industry Development Strategy, Defence has commenced the process to update the Defence Policy for Industry Participation and procurement reform initiatives to ensure Defence and industry are better positioned to deliver the required capabilities within reduced timeframes. These reforms will directly support the implementation of the ANAO's recommendations relating to improvement of administrative arrangements to enable identification and monitoring of Defence's industry policies enabled through its contract frameworks.

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.

Policy design

- Successful policy implementation requires senior management oversight and implementation planning to set clear responsibilities and timeframes for the delivery of agreed activities.
- Prerequisites or threshold activities should be clearly identified and delivered in accordance with an agreed implementation plan. Appropriate sequencing provides for a solid foundation in the later stages of delivery and the timely establishment of administrative arrangements, such as:
  - clear and consistent policies, templates and guidance materials;
  - effective IT system controls to ensure compliance with policy requirements;
  - reliable assurance reporting against a standards-based assurance framework; and
  - effective governance oversight and reporting arrangements to monitor the impact of policy and the achievement of intended objectives.

The Auditor-General
Auditor-General Report No.2 2024–25
Performance Audit

Defence’s Management of ICT Systems Security Authorisations

Department of Defence

Australian National Audit Office

Audit snapshot

Auditor-General Report No.2 2024–25

Defence's Management of ICT Systems Security Authorisations

Why did we do this audit?

- Malicious cyber activity represents a key risk for the Department of Defence (Defence).
- Protective Security Policy Framework (PSPF) Policy 11 outlines how ICT systems can be protected through authorisation activities to support the delivery of government business.
- This audit was conducted to provide assurance to the Parliament on Defence's arrangements for the management of its ICT systems authorisations.

Key facts

- The Defence Security Principles Framework (DSPF) requires that 'all Defence ICT systems must be authorised prior to processing, storing or communicating official information'.
- The DSPF provides for system authorisation decisions to be escalated to more senior personnel based on the system's assessed residual risk level.

What did we find?

- Defence's arrangements to manage the security authorisation of its ICT systems have been partly effective.
- Defence's arrangements for system authorisation have not been regularly reviewed and do not reflect current PSPF requirements.
- Defence's reporting did not comply with DSPF requirements, omitted key system authorisation data, and indicated a more optimistic outlook than was reflected in other Defence documentation.
- Defence did not comply with the PSPF and DSPF system authorisation requirements for the five case studies examined in the audit.

What did we recommend?

- There were eight recommendations to Defence aimed at improving: the review and update of assessment arrangements; training; the quality of supporting information; assurance and reporting arrangements; and compliance with authorisation requirements.
- Defence agreed to the eight recommendations.

285 days

was the average time to process system authorisations from September 2020 to September 2021.

5%

of Defence's ICT systems have been registered in Defence's ICT authorisation management system as at June 2024.

47%

of those ICT systems registered have been recorded as 'Expired' or 'No accreditation' as at August 2024.

Summary and recommendations

Background

1. The security of government information and communications technology (ICT) systems, networks and data supports Australia's social, economic and national security interests as well as the privacy of its citizens. Malicious cyber activity has been identified as a significant threat affecting Australians, exacerbated by low levels of cyber maturity across many Australian Government entities.[1]

2. The Department of Defence's (Defence's) mission and purpose is to defend Australia and its national interests in order to advance Australia's security and prosperity. Defence's 2022 Cyber Security Strategy states that 'Malicious cyber activity now represents one of Defence's most critical risks.'[2]

3. The Protective Security Policy Framework (PSPF) was introduced in 2010 to help Australian Government entities protect their people, information and assets, both at home and overseas. The PSPF sets out the government's protective security policy approach and is comprised of 16 core policies.[3] PSPF Policy 11 *Robust ICT systems* requires that:

> Entities **must** [emphasis in original] only process, store or communicate information and data on an ICT system that the determining authority (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation.[4]
>
> When establishing new ICT systems, or implementing improvements to an existing system, the decision to authorise (or reauthorise) a system to operate **must** [emphasis in original] be based on the Information Security Manual's [ISM] six step risk-based approach for cyber security.[5]

4. Defence has established the Defence Security Principles Framework (DSPF) to support compliance with the requirements of the PSPF. The DSPF outlines Defence's requirements for ICT

---

1 Australian Government, *2023–2030 Australian Cyber Security Strategy* [Internet], 22 November 2023, p. 43, available from https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf [accessed 13 March 2024].

2 Department of Defence, *Defence Cyber Security Strategy* [Internet], 31 August 2022, p. 5, available from https://www.defence.gov.au/sites/default/files/2022-08/defence-cyber-security-strategy.pdf [accessed 13 March 2024].
A paper presented to Defence's Enterprise Business Committee in October 2021, seeking approval for the Cyber Security Strategy noted that: Defence's cyber security governance is 'fragmented and uncoordinated'; 'Defence's cyber security maturity ratings consistently fall below target scores'; and Defence has 'many legacy systems requiring disproportionate attention'.

3 Department of Home Affairs, *Protective Security Policy Framework* [Internet], available from https://www.protectivesecurity.gov.au/policies [accessed 3 April 2024].
The PSPF is not specifically legislated. The PSPF is underpinned by the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requirements to govern an entity in a manner that is 'not inconsistent' with Australian Government policies and promote the proper use and management of public resources.

4 For systems with a classification of Top Secret, the Authorising Officer is the Director-General of the Australian Signals Directorate, or their delegate. As discussed at paragraph 1.25, the authorisation of Top Secret systems is outside the scope of this audit.

5 While PSPF Policy 11 and its associated requirements were introduced as part of a revision to the PSPF in 2018, the requirement for entities to authorise ICT systems based on the acceptance of residual risks has existed since the introduction of the ISM in 2009.

assessment and authorisation including that 'all Defence ICT systems must be authorised prior to processing, storing or communicating official information'.

Rationale for undertaking the audit

5. Through its 2022 Cyber Security Strategy, Defence has recognised that 'Malicious cyber activity now represents one of Defence's most critical risks.' Robust ICT systems protect the confidentiality, integrity and availability of the information and data that entities process, store and communicate. PSPF Policy 11 outlines how entities can safeguard ICT systems through assessment and authorisation activities to support the secure and continuous delivery of government business.

6. Questions regarding Defence's system authorisation process were raised at hearings of the Senate Foreign Affairs, Defence and Trade Legislation Committee in June 2021, including in relation to:

- Defence's use of provisional authorisations beyond 12 months for systems where security concerns have not been sufficiently addressed;
- deficiencies in Defence's processes for identifying and assessing risks as part of the authorisation process; and
- DSPF compliance with the Information Security Manual (ISM).

7. This audit was conducted to provide assurance to the Parliament on Defence's arrangements for the management of ICT systems security authorisations.[6]

Audit objective and criteria

8. The audit objective was to assess the effectiveness of the Department of Defence's arrangements to manage the security authorisation of its ICT systems.

9. To form a conclusion against this objective, the following high-level criteria were adopted.

- Does Defence have fit-for-purpose arrangements for the security authorisation of its ICT systems?
- Has Defence implemented its arrangements for the security authorisation of its ICT systems?

Engagement with the Australian Signals Directorate

10. Independent timely reporting on the implementation of the cyber security policy framework supports public accountability by providing an evidence base for the Parliament to hold the executive government and individual entities to account. Previous ANAO reports on cyber security have drawn to the attention of Parliament and relevant entities the need for change in entity implementation of mandatory cyber security requirements, at both the individual entity and framework levels.

6 The Hon Brendan O'Connor MP and Mr Tim Watts MP requested an audit into Defence's use of provisional authorisations on 5 June 2021. See Australian National Audit Office, *The use of provisional ICT accreditation within Defence* [Internet], 5 June 2021, available from https://www.anao.gov.au/work/request/the-use-provisional-ict-accreditation-within-defence [accessed 4 April 2024].

11. In preparing audit reports to the Parliament on cyber security in Australian Government entities, the interests of accountability and transparency must be balanced with the need to manage cyber security risks. The Australian Signals Directorate (ASD) has advised the ANAO that adversaries use publicly available information about cyber vulnerabilities to more effectively target their malicious activities.

12. The extent to which this report details the cyber security vulnerabilities of Defence was a matter of careful consideration during the course of this audit. To assist in appropriately balancing the interests of accountability and potential risk exposure through transparent audit reporting, the ANAO engaged with ASD to better understand the evolving nature and extent of risk exposure that may arise through the disclosure of technical information in the audit report. This report focusses on matters material to the audit findings against the objective and criteria.

Conclusion

13. Defence's arrangements to manage the security authorisation of its ICT systems have been partly effective. Systems have not been authorised in a timely manner and were assessed through processes that did not consistently comply with Protective Security Policy Framework (PSPF) requirements.

14. Defence's arrangements for the security authorisation of its ICT systems are partly fit for purpose. Defence's policies, frameworks and processes to support system assessment and authorisation have not been regularly reviewed or updated to align with PSPF and Defence Security Principles Framework (DSPF) requirements. These policy and process documents are internally inconsistent. Defence has not established training to ensure that key personnel involved in the authorisation process remain up-to-date with changing cyber security requirements in the Information Security Manual (ISM) and PSPF.

15. Defence has partly implemented arrangements for the security authorisation of its ICT systems. Defence's data on its system assessments and authorisations is incomplete and indicates that System Owner obligations to obtain and maintain authorisation of their systems are not being fulfilled.

16. There were deficiencies in relation to Defence's monitoring and reporting arrangements, including non-compliance with DSPF reporting requirements. Key information on the system authorisation status of Defence's systems was omitted from Defence's reporting, including not addressing a request from the Minister for Defence to include metrics in reporting on unapproved ICT systems within Defence. Defence's internal and external reporting on its assessments indicated a more optimistic outlook than was otherwise reflected in other internal Defence documentation. Across the ICT systems examined in case studies, deficiencies included: the absence of key data and mandatory security documentation; no evidence of assessment of control implementation; and deficiencies in the peer review process.

Supporting findings

Defence's arrangements for the security authorisation of its ICT systems

17. Defence has not appropriately maintained its policy and governance framework for the authorisation of its ICT systems. When the DSPF was implemented in July 2018, some sections

were not complete, with key authorisation roles listed but not defined for 13 of the 14 Defence Services and Groups listed. These roles remained undefined until a May 2024 review of the DSPF. Prior to the May 2024 update, DSPF Principle 23 and DSPF Control 23.1 had not been updated since July 2020. This meant that key changes to the mandatory requirements in PSPF Policies 10 and 11 between August 2020 and February 2022 — such as the introduction of the 'Essential Eight' and the ISM six-step process for system assessment and authorisation — were not reflected in the DSPF until 10 May 2024. (See paragraphs 2.3–2.25)

18. Directives, instructions, and policies issued by the Australian Defence Force (ADF) services for ICT authorisations for Army, Navy and Air Force systems contain provisions that are either not consistent with or not permitted by the requirements of the DSPF, or PSPF Policy 11. These provisions have allowed for exemptions to Defence's system authorisation process that are not permitted under the DSPF or PSPF. (See paragraphs 2.26–2.38)

19. A key supporting framework, the *Defence ICT Certification and Accreditation Framework* (DICAF) — developed to ensure consistency in the authorisation process for all Defence ICT systems that process, store or communicate official, sensitive or classified information — has been in draft since December 2015. As at May 2024, the DICAF remains incomplete with a placeholder remaining for a key section that was to be developed on the assessment and authorisation process. In response to shortcomings identified in the DICAF by an internal audit in May 2020, Defence developed a separate 'Assessment and Authorisation Framework' document in December 2021. The framework was approved by Defence's Chief Information Security Officer (CISO) in February 2024 and released in May 2024. (See paragraphs 2.39–2.51)

20. Defence does not have an up-to-date set of consolidated guidance to support the implementation of its framework in a consistent manner across the organisation. Defence's assessment and authorisation process guidance is internally inconsistent and a number of supporting templates have not been finalised or are outdated. Separate instructions, directives and policies exist for the Army, Navy and Air Force, which include some requirements that are inconsistent with Defence's assessment and authorisation process, the DSPF and PSPF. (See paragraphs 2.52–2.73)

21. Defence has not established training to ensure that Security Assessors remain up-to-date on evolving cyber security requirements, instead relying on peer review and Assessment Authority review to mitigate any 'deficiencies in knowledge'. Deficiencies were identified in Defence's implementation of the peer review process and Defence does not undertake assurance activities to monitor the extent to which training is completed. The absence of a formalised training approach to support the implementation of DSPF requirements for the assessment and authorisation of ICT systems creates a risk that systems are not being authorised as intended. Defence data on ICT system authorisations shows that 47 per cent of its systems have a status of either 'Expired' or 'No accreditation', indicating that System Owner obligations in respect to obtaining and maintaining the authorisation of their systems are not being met. (See paragraphs 2.74–2.93)

Implementation of arrangements for the security authorisation of Defence's ICT systems

22. Defence's data indicates that the obligations of System Owners to obtain and maintain the authorisation of their systems are not being fulfilled. (See paragraphs 3.5–3.26)

23. Defence self-assesses and reports annually on its compliance with PSPF Policy 11 and has established governance and internal reporting requirements for DSPF controls, including DSPF Control 23.1 *ICT Certification and Accreditation.* Deficiencies in Defence's reporting include that:

- Defence has not reported on the authorisation status of ICT systems at an enterprise level since 2018–19 in its PSPF and DSPF reporting (a key indicator of compliance against DSPF Control 23.1 and PSPF Policy 11);
- Defence's PSPF and DSPF reporting is not consistent with, and does not reflect, other information available within Defence on the assessment and authorisation of its ICT systems; and
- Defence has not complied with the DSPF requirement to provide individual Control Owner reports to the Defence Security Committee since 2019–20. (See paragraphs 3.27–3.68)

24. Defence has not briefed the minister on its ICT assessment and authorisation activities in the last three years. In September 2019, the minister requested that Defence include a metric on the reduction of unapproved systems in an 'ICT reform stream report'. Defence did not address this request. (See paragraphs 3.69–3.73)

25. Defence has not consistently complied with the requirements of its assessment and authorisation process. For example, for all five systems examined:

- key supporting data had not been entered in Defence's ICT authorisation management system, and mandatory security documentation had not been provided to the Security Assessors;
- Defence was unable to substantiate that document reviews and control implementation assessments took place; and
- there were shortcomings in the peer review process, including not identifying that mandatory security documentation was missing, and not identifying inaccuracies and errors in Risk Assessments. (See paragraphs 3.74–3.90)

26. There were instances where systems had been re-authorised based on the re-authorisation triggers in the DSPF. These re-authorisations were not always granted prior to authorisation expiry. (See paragraphs 3.91–3.100)

Recommendations

Recommendation no. 1
Paragraph 2.24

The Department of Defence ensure that DSPF roles and requirements for system assessment and authorisation are complete, current, and regularly reviewed for alignment with the PSPF and Group/Service appointments.

Department of Defence response: *Agreed.*

Recommendation no. 2
Paragraph 2.72

The Department of Defence conducts a review of, and updates, its assessment and authorisation process documentation to ensure:

(a) alignment with current DSPF and PSPF requirements;

(b) consistency across all internal guidance documents, including those developed by the ADF Services; and

(c) that any internal inconsistencies within individual guidance documents are eliminated.

Department of Defence response: *Agreed.*

Recommendation no. 3
Paragraph 2.89

The Department of Defence:

(a) implements improved training and awareness raising activities to ensure that key personnel involved in the assessment and authorisation process are aware of their obligations under the PSPF and DSPF, and remain up-to-date with evolving cyber security requirements; and

(b) implements a framework to monitor and report on the completion of training and awareness raising activities.

Department of Defence response: *Agreed.*

Recommendation no. 4
Paragraph 3.25

The Department of Defence develops and implements processes to ensure that information entered into its ICT authorisation management system is complete, accurate, and supports effective monitoring of ICT system authorisations.

Department of Defence response: *Agreed.*

Recommendation no. 5
Paragraph 3.45

The Department of Defence:

(a) implement enterprise-wide assurance arrangements to support the effective implementation of DSPF system authorisation requirements; and

(b) implement arrangements to ensure that deficiencies and non-compliance identified through Service assurance activities relating to system authorisations are addressed and rectified.

Department of Defence response: *Agreed.*

Recommendation no. 6
Paragraph 3.67

The Department of Defence implement arrangements to ensure reporting to senior Defence leadership on compliance with system authorisation requirements under the PSPF and DSPF is comprehensive, accurate, and based on available data.

Department of Defence response: *Agreed.*

Recommendation no. 7
Paragraph 3.72

The Department of Defence:

(a) ensures that relevant ministers are provided with timely and accurate advice on key issues and risks relating to Defence's ICT security authorisations and its compliance with the PSPF; and

(b) provides regular (at least annual) updates to relevant ministers to support oversight for improvements to its

assessment and authorisation policies, frameworks and processes.

Department of Defence response: *Agreed.*

Recommendation no. 8
Paragraph 3.98

The Department of Defence implements arrangements to ensure that PSPF requirements, DSPF requirements and Defence's assessment and authorisation process are complied with, including:

(a) ensuring that all required documentation has been completed prior to system assessment and authorisation;

(b) documenting the approval and review of mandatory supporting documentation;

(c) conducting and documenting assessments of the implementation and effectiveness of controls and provisional authorisation conditions against all relevant ISM and DSPF controls; and

(d) ensuring systems are proactively monitored against the conditions for re-authorisation.

Department of Defence response: *Agreed.*

Summary of the Department of Defence's response

27. The proposed audit report was provided to the Department of Defence. Defence's summary response is provided below, and its full response is included at Appendix 1. Improvements observed by the ANAO during the course of this audit are listed in Appendix 2.

> Defence welcomes the Auditor-General Report: *Defence's Management of ICT Security Authorisation*. Defence agrees to the eight recommendations aimed at improving Defence's Cyber Security Assessment and Authorisation Framework to more effectively govern and monitor the authorisation of ICT systems and networks and control cyber-related ICT risk.
>
> Defence is committed to strengthening and standardising our approach to safeguarding data from cyber threats and ensuring the secure operation of our ICT systems to protect the continuous delivery of Defence outcomes. Defence is currently reviewing its Cyber Security Assessment and Authorisation Framework, along with the associated policies, practices and processes, as part of Defence's wider initiative to uplift cyber security governance and its cyber risk management framework. This includes an overhaul of several pertinent Defence Security Principles Framework policies, which are undergoing review, along with a program to drive Essential 8 Maturity.

Key messages from this audit for all Australian Government entities

28. 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.

Governance and risk management

- Policy and guidance documentation should be kept up-to-date, especially when it relates to activities to manage key entity risks. Periodic review of documentation helps maintain its fitness-for-purpose and alignment with Commonwealth standards.

Performance and impact measurement

- Accurate and transparent monitoring and reporting on compliance supports effective decision-making and accountability. Monitoring and reporting should be supported by data that is accurate and complete.

The Auditor-General
Auditor-General Report No.1 2024–25
Performance Audit

Defence’s Procurement and Implementation of the myClearance System

Department of Defence

Australian National Audit Office

Audit snapshot

Auditor-General Report No.1 2024–25

Defence's Procurement and Implementation of the myClearance System

Why did we do this audit?

- The new whole-of-government vetting system, myClearance, went live on 28 November 2022. By February 2023, the extent of the user issues encountered after the system's introduction was the subject of parliamentary interest.
- This audit was identified as a 2023–24 audit priority by the Joint Committee of Public Accounts and Audit.
- The audit provides assurance to the Parliament on the effectiveness of the Department of Defence's (Defence) procurement and implementation of the myClearance system.

Key facts

- A total acquisition budget of $138.6 million for the delivery of a base capability (in Quarter 4 2022) and a 'continuous assessment' module (in Quarter 4 2023) was approved by government in December 2020.
- By July 2023, 87 per cent of the total acquisition budget had been expended and delivery of the continuous assessment module remained ongoing.
- In November 2023, Defence recommended, and government agreed to de-scope the: continuous assessment; automated risk sharing; use of artificial intelligence; and enhanced interface functionalities of the myClearance system.

What did we find?

- Defence's procurement and implementation of the myClearance system was partly effective.
- Defence's planning activities were largely effective. Defence's governance, oversight and reporting arrangements were not implemented effectively and did not support informed, risk-based decision-making.
- The procurement processes for the systems integrator and project delivery partner were not conducted in a manner consistent with Defence's procurement policy or the intent of the Commonwealth Procurement Rules (CPRs).
- Initial implementation of the system was not effective. Defence's remediation efforts, since the system went live, have achieved progressive improvements. In November 2023, Defence advised government that the system will not deliver the full functionality as approved by government in December 2020.

What did we recommend?

- There were two recommendations made to improve Defence's management of risk and the security of the myClearance system.
- The Department of Defence has agreed to the two recommendations.

$138.6 m

the approved acquisition budget for the myClearance system.

60%

of the acquisition budget was for systems integration services.

107,249

security clearances processed in the myClearance system to 9 May 2024.

Summary and recommendations

Background

1. Security vetting involves the assessment of an individual's suitability to hold a security clearance at a particular level. Australian Government employees and contractors require a security clearance to access classified resources, which can relate to Australia's national security, economic and other interests.[1] The security vetting and clearance process is an important risk mitigation activity intended to protect the national interest, which can also affect an individual's employment and the business operations of entities if not managed effectively or in a timely manner.

2. The Australian Government Security Vetting Agency (AGSVA) is part of the Department of Defence (Defence) and provides security clearance assessments as a whole-of-government service. In February 2014, Defence identified the need for long-term and potentially significant investment in ICT solutions because the existing system used by AGSVA to process security clearances, the Personnel Security Assessment Management System (PSAMS), did not have the 'functionality needed for the future'. The February 2016 Defence *Integrated Investment Program* (IIP) subsequently outlined a need for 'expanded security vetting' as one of the 'principal areas of focus' for Defence.[2]

3. In October 2016, the Australian Government agreed to a suite of reforms to improve government entities' management of the threat posed by malicious insiders, which included upgrading AGSVA's ICT system.[3]

Vetting Transformation Project

4. The 'Defence and Security Vetting Services 20/20 Reform Program' was established in December 2016 and consisted of four workstreams: vetting; security policy, services and advice; security governance, assurance and reporting; and cultural change. The objectives for the vetting workstream included delivering: a new vetting security business model; a supporting ICT system; and relevant training, communications and change management activities.

5. The Vetting Transformation Project was established to deliver the vetting workstream objectives, including the design and implementation of a new system that:

---

1 The requirement for and purpose of security vetting is discussed further at paragraph 1.19.

2 Department of Defence, *2016 Defence Integrated Investment Program*, February 2016, p.41. The Integrated Investment Program (IIP) is a ten-year expenditure plan covering activities and projects that have been approved for inclusion in the IIP by the government. An IIP provision sets out what funding has been provisioned (including for acquisition and sustainment), whether the funding is approved or unapproved by the government for the project and release of funds, and in which financial years the funding is currently allocated to. The 2016 IIP was released with the *2016 Defence White Paper.*

Two programs within the key enabler capability stream of the 2016 IIP are related to 'expanded security vetting'. A security systems modification program was allocated a budget of between $100 million to $200 million, to be implemented over the 2018 to 2025 period. A secure and unified computer and storage transformation program was allocated a budget of between $750 million and $1 billion, to be implemented between 2020 and 2030.

3 The previous ICT system was comprised of: the ePack; the Personnel Security Assessment Management (PSAMS) database; and a security officer dashboard.

- provides sponsoring entities with information on identified risk factors associated with individual clearance holders;
- increases automation of clearance decision-making and data collection (including across other government holdings, and online social-media information); and
- supports continuous assessment of security risk.[4]

Previous ANAO reports

6. The ANAO previously reviewed Defence's performance in providing security vetting services through AGSVA in the following performance audits.

- Auditor-General Report No.45 2014–15 *Central Administration of Security Vetting,* which was presented for tabling in Parliament in June 2015. The audit conclusion was that the performance of centralised vetting had been mixed and government expectations of improved efficiency and cost savings had not been realised.[5]
- Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security*, which was presented for tabling in May 2018. The audit conclusion was that the effectiveness of personnel security arrangements for managing insider threats had been reduced by AGSVA not implementing the government's policy direction to share information with client entities on identified personnel security risks. The report also observed that AGSVA planned to realise the necessary process improvements through the procurement of a new ICT system, expected to be fully operational in 2023.[6]

Rationale for undertaking the audit

7. The ANAO undertook this audit, and previous (2015 and 2018) audits of Defence's provision of security vetting services through AGSVA, as effective personnel security arrangements underpin the protection of the Australian Government's people, information and assets. Previous audits identified deficiencies in AGSVA's information systems. In the context of the Joint Committee of Public Accounts and Audit's (JCPAA) inquiry into the ANAO's 2018 audit, Defence advised the JCPAA that a project to build a new ICT system had received first-pass approval in April 2018, with delivery of the 'initial operating capability' (the base capability) expected in late 2020.[7]

8. The base capability of the new system was introduced on 28 November 2022. By February 2023, the extent of user issues experienced after the system 'went live' were the subject of parliamentary interest. This audit provides independent assurance to the Parliament on the

4 Auditor-General Report No.38 2017–18, *Mitigating Insider Threats through Personnel Security*, ANAO, Canberra, 2018, para 2.62, available from https://www.anao.gov.au/work/performance-audit/mitigating-insider-threats-through-personnel-security.

5 Auditor-General Report No.45 2014–15, *Central Administration of Security Vetting,* ANAO, Canberra, 2015, para 13, available from https://www.anao.gov.au/work/performance-audit/central-administration-security-vetting.

6 Auditor-General Report No.38 2017–18, *Mitigating Insider Threats through Personnel Security*, paragraph 7.

7 Commonwealth, Official Committee Hansard, Joint Committee of Public Accounts and Audit, *Personnel security, domestic passenger screening – Auditor-General's reports 38 and 43 (2017–18)*, Friday 17 August 2018, pp.8-9, available from https://parlinfo.aph.gov.au/parlInfo/download/committees/commjnt [accessed 16 May 2024].

effectiveness of Defence's procurement and implementation of the new ICT system, now known as myClearance, and Defence's remediation progress to date.

Audit objective and criteria

9. The objective of the audit was to assess the effectiveness of Defence's procurement and implementation of the myClearance system to date.

10. To form a conclusion against the audit objective the following high-level criteria were adopted.

- Did Defence plan effectively and establish fit for purpose governance, oversight and reporting arrangements?
- Was Defence's implementation of the system effective and supported by procurement processes conducted in accordance with the Commonwealth Procurement Rules (CPRs)?

11. The audit focused on the procurement of the project approval and support services provider (Deloitte), the prime systems integrator (Accenture), the organisational change management partner (KPMG) and the project delivery partner (VOAK Group). The audit also considered the arrangements used to procure the hardware and software components of the myClearance system, and other services to manage the delivery of the Vetting Transformation Project. The audit did not examine Defence's administration or management of its contracts with the service providers.

Conclusion

12. Defence's procurement and implementation of the myClearance system to date has been partly effective. The full functionality of the system will not be delivered as key elements, including the continuous assessment, automated risk-sharing and enhanced interface functionalities, were de-scoped from the project in November 2023.

13. Defence's planning activities were largely effective. Early planning work in 2016 and 2017 focused on industry engagement and assessing the market's ability to deliver and integrate the new IT system into Defence's ICT environment. Work to refine the user and system requirements in mid-2018 was not informed by other government entities or stakeholders. Defence designed governance, oversight and reporting arrangements in line with the requirements of its Capability Life Cycle framework. The project governance arrangements were not implemented effectively and there was a lack of clarity on the purpose of and relationship between the various decision-making forums. Project reporting did not support informed, risk-based decision-making as project risks and issues were not clearly communicated to Defence leadership.

14. Defence's procurement processes were partly effective. The processes to engage project approval and support services and the organisational change management partner were conducted in line with the Commonwealth Procurement Rules (CPRs). The process to engage the prime systems integrator was not consistent with the CPRs. The tender documentation included a list of mandatory products referring to trade names and producers — an approach that did not comply with Defence's procurement policy framework. Defence's conduct of the 'Analysis of Alternatives' in early 2020 resulted in material changes to the technical solution, schedule and delivery approach and provided opportunities to the preferred supplier that were not provided

to other prospective suppliers. Defence's approach to engaging the Project Delivery Partner in 2022 did not comply with Defence's Accountable Authority Instructions or the intent of the CPRs.

15. Defence's implementation of the myClearance system has been partly effective. Identified risks and issues were not resolved in a timely manner. Data cleansing and migration activities were not effective. Testing processes were truncated and were not conducted in line with agreed testing plans or Defence guidance. To address the issues encountered after the core vetting system went live in November 2022, Defence established the myClearance taskforce in February 2023. Defence's remediation activities have progressively improved the performance of the system since it went live. In July 2023, Defence advised government that it had delivered a system that largely met the initial operating capability requirements. In November 2023 Defence advised government that the myClearance system would not deliver the full functionality as approved in December 2020.

Supporting findings

Effectiveness of planning activities

16. Defence conducted early planning activities between late 2016 and early 2018. Industry engagement and market research was undertaken to assess the market's ability to design, build and integrate a new IT system into Defence's ICT environment. Workshops and forums held to refine the user requirements and technical components in June 2018 did not include external stakeholders such as other government entities with ICT systems that AGSVA's new vetting system would need to integrate or interface with. (See paragraphs 2.7 to 2.29)

17. The financial and technical risks associated with the planned procurement were assessed. To mitigate some of the identified risks, a list of mandatory products referring to trade names and producers was included in Defence's tender documentation for the IT solution to be delivered by the systems integrator. As a result, the design of the procurement:

- did not comply with Defence's procurement policy framework and was inconsistent with the Commonwealth Procurement Rules (CPRs);
- reduced the opportunity for suppliers to propose alternative solutions based on 'functional and performance requirements' that may have met Defence's requirements; and
- introduced critical dependencies that increased the integration and schedule risks of the project. These risks were not effectively managed or communicated to senior Defence leadership or government. (See paragraphs 2.30 to 2.52)

Governance, oversight and reporting arrangements

18. Defence established governance, oversight and reporting arrangements for the Vetting Transformation Project in accordance with its Capability Life Cycle Manual — a framework that was designed to govern Defence's acquisition of complex military equipment and materiel. These arrangements were not implemented effectively. (See paragraphs 2.63 to 2.79)

19. Reporting to decision-making forums accurately assessed the risks and issues that contributed to the problems experienced after the system 'went live'. The impacts of those risks

and issues on the expected functionality and capability of the system were not clearly communicated to Defence leadership. (See paragraphs 2.86 to 2.96)

20. Successive reviews, including independent assurance reviews found that project governance arrangements were not 'formally defined and maintained' and there was a lack of clarity on the purpose of and relationship between each forum within the governance model. At March 2024, Defence had commenced a program of work to address the identified governance issues, including the implementation of a new governance model for the project. (See paragraphs 2.82 to 2.84 and 2.103 to 2.112)

Procurement processes

21. The processes to engage project approval and support services and the organisational change management partner were conducted in accordance with the CPRs. For the prime systems integrator (PSI) procurement, processes such as initial screening, evaluation, value for money assessment, and additional clarification activities were compliant with CPR requirements. Key shortcomings in the design of the PSI procurement resulted in the conduct of activities that were not consistent with the CPRs. These activities involved material changes to the technical solution, schedule and delivery approach and provided opportunities to the preferred supplier that were not provided to other prospective suppliers. These opportunities enabled the preferred supplier to develop a 'solution to a budget' and submit costings for work it did not originally tender for. (See paragraphs 3.15 to 3.44)

22. Defence did not comply with its Accountable Authority Instructions for the procurement of the Project Delivery Partner in June 2022. Up to 85 per cent of the project management and other specialist support services were engaged through approaches to single suppliers, selected from a panel on each occasion. This approach was technically compliant with the CPRs but was not consistent with their intent — to drive value for money through competition. (See paragraphs 3.48 to 3.56)

Implementation of the system

23. Identified risks and issues were not resolved in a timely manner and cumulative delays in providing Government Furnished Materials to the Prime Systems Integrator gave rise to risks impacting the critical path of the project. These risks were realised, reducing the time available to test the system as required prior to the core vetting system (the base capability) going live on 28 November 2022. (See paragraphs 3.63 to 3.66, 3.70 to 3.72, and 3.84 to 3.90)

- Data cleansing and migration activities were not conducted effectively or completed in a timely manner. Representative data (production data) was not used for testing as planned. The impacts arising from these issues on the functionality and capability of the system were not clearly communicated to decision-makers. (See paragraphs 3.103 to 3.110)
- Testing activities were truncated and were not conducted in line with agreed testing plans or in a manner consistent with Defence guidance. Testing activities that were to be conducted sequentially were conducted in parallel. (See paragraphs 3.111 to 3.123)
- Defence does not have a program in place to monitor and review privileged user activity and does not have a process to periodically revalidate user accounts for the myClearance system. (See paragraphs 3.91 to 3.100)

24. Throughout 2023, Defence's myClearance taskforce achieved progressive improvements to the core vetting system. In November 2023, Defence recommended that the government agree to de-scoping the: continuous assessment; automated risk sharing; use of artificial intelligence; and enhanced interfaces from the myClearance system. As a consequence, the myClearance system will not deliver the desired capability uplift or provide the full functionality advised to government in December 2020. (See paragraphs 3.135 to 3.139)

Recommendations

25. The ANAO has made two recommendations to improve risk management for complex high value ICT projects and manage and maintain the security of the system.

Recommendation no. 1
Paragraph 2.53

The Department of Defence ensure that risk management plans, comprising a risk appetite statement and risk tolerances, are developed, implemented and maintained for its complex, high value ICT projects.

Department of Defence response: *Agreed.*

Recommendation no. 2
Paragraph 3.101

The Department of Defence develop and implement a program of work to periodically revalidate user access and monitor privileged user accounts to ensure that management of the myClearance system complies with the requirements of the Information Security Manual.

Department of Defence response: *Agreed.*

Summary of the Department of Defence's response

26. The proposed audit report was provided to the Department of Defence. Defence's summary response is provided below, and its full response is included at Appendix 1. Improvements observed by the ANAO during the course of this audit are listed in Appendix 2.

> Defence acknowledges the Auditor-General's findings that the implementation of the myClearance system was partly effective. Defence is committed to strengthening procurement and governance arrangements, ensuring important projects are delivered in the best interests of Australia's national security.
>
> Defence has achieved substantial improvements in security clearance processing since the system launched. Following the introduction of myClearance in November 2022, over 110,000 clearances have been processed, with over 75,000 clearances completed in the myClearance system during 2023–24. Vetting timeframes for all clearance levels are also being consistently met.
>
> Defence is committed to increasing ICT project risk oversight and management through three robust lines of assurance to ensure decision makers are well informed of emerging risks and potential impacts. The methodology includes:
>
> - Establishing robust first-line assurance for ICT projects prior to progressing through gate decisions, ensuring all mandatory project artefacts are complete and performance milestones are achieved;

- Increasing second-line assurance, assessing ICT project governance implementation and the end-to-end business solution; and
- Continuing third-line enterprise level objective assessment of adequacy, effectiveness and efficiency of governance, performance and risk management.

Defence is confident this holistic approach to oversight and assurance will enable active identification, robust management and reporting of risks and opportunities.

Key messages from this audit for all Australian Government entities

27. 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.

Governance and risk management

- Reporting on technical issues and risks should be clearly communicated to senior leaders and decision makers in plain English and in terms of the anticipated impact on the functionality or capability of the system.

The Auditor-General
Auditor-General Report No.47 2023–24
Performance Audit

Defence’s Management of Contracts for the Supply of Munitions — Part 1

Department of Defence

Australian National Audit Office

Audit snapshot

Auditor-General Report No.47 2023–24

Defence's Management of Contracts for the Supply of Munitions — Part 1

Why did we do this audit?

- The implementation of a Guided Weapons and Explosive Ordnance (GWEO) enterprise was announced as a key government priority in the 2023 *Defence Strategic Review*, and the domestic manufacture of GWEO and munitions was one of seven Sovereign Defence Industrial Priorities announced by the Australian Government in the *Defence Industry Development Strategy* in April 2024.
- This audit provides independent assurance to the Parliament on Defence's establishment of a 10-year agreement with Thales from July 2020 for the continued management and operation of the Mulwala and Benalla facilities. It builds on previous ANAO work examining Defence's management of the facilities over time.

Key facts

- The Mulwala and Benalla facilities are Commonwealth-owned and have been operated by a third party (Thales Australia) since 1999.
- The current contract, the Strategic Domestic Munitions Manufacturing (SDMM) contract, replaced a five-year interim contract, which was established after a competitive process was terminated in 2014.

What did we find?

- Defence's conduct of the sole source procurement for the operation and maintenance of the Mulwala and Benalla facilities beyond June 2020 was partly effective.
- Defence's planning for the operation and maintenance of the facilities beyond the expiry of the 2015–20 interim contract was partly effective.
- Defence's conduct of the sole source procurement process to establish the 2020–30 contractual arrangements was partly effective.
- Defence's management of probity was not effective and there was evidence of unethical conduct.

What did we recommend?

- There were eight recommendations to Defence aimed at improving: procurement planning; advice to decision-makers; management of probity risks and issues; compliance with record keeping requirements; and traceability of negotiation directions and outcomes.
- Defence agreed to the eight recommendations.

$1.2 bn

contract price (GST exclusive) at 31 March 2024.

$108 m

value (GST inclusive) of reported contract variations (relating to survey and quote work orders) at 19 June 2024.

$225 m

minimum munitions order value (GST exclusive) under the contract.

Summary and recommendations

Background

1. The Mulwala facility in New South Wales is the sole remaining manufacturing site of military propellants and high explosives in Australia. The nearby munitions facility at Benalla, Victoria, uses some of the output of the Mulwala facility in its operations. Both facilities are owned by the Commonwealth and operated by a third party, Australian Munitions, a wholly owned subsidiary of Thales Australia (Thales).[1] Thales has managed and operated the facilities at Benalla and Mulwala under several different contractual arrangements since 1999 (outlined in Appendix 3).

2. The Australian Government announced on 29 June 2020 that the Department of Defence (Defence) had signed a new 10-year agreement valued at $1.2 billion with Thales for the continued management and operation of the Mulwala and Benalla facilities.[2] The agreement was intended to provide surety of supply of key munitions and components for the Australian Defence Force (ADF) and maintain a domestic munitions manufacturing capability. The agreement took effect on 1 July 2020 and resulted from a complex multi-year sole source procurement begun in 2016. The sole source procurement followed a terminated competitive procurement process undertaken between 2009 and 2014.

3. The Australian Government also announced on 29 June 2020 a new contract between the Commonwealth and NIOA Munitions (NIOA) for a tenancy at the Benalla munitions factory.[3] This agreement was to establish NIOA as a tenant alongside Thales and provide opportunities for domestic manufacturing while enhancing supplies of key munitions for Defence.[4]

4. On 24 April 2023, the Australian Government released a public version of the final report of the *Defence Strategic Review* (DSR).[5] It referenced the continuing importance of advanced munitions manufacturing, stating that the immediate focus must be on consolidating ADF guided weapons and explosive ordnance (GWEO) needs, establishing a domestic manufacturing capability, and the acceleration of foreign military and commercial sales. The report further outlined that, to

1 For convenience, this report refers to Australian Munitions/Thales Australia as Thales. Australian Munitions commenced trading on 2 November 2012. Prior to this, Thales managed and operated the facilities through ADI Limited, which became a wholly owned subsidiary of Thales Australia in 2006.

2 Minister for Defence and Minister for Defence Industry, 'Securing domestic manufacturing capability for Australian Defence Force munitions', joint media release, 29 June 2020, available from https://www.minister.defence.gov.au/media-releases/2020-06-29/securing-domestic-manufacturing-capability-australian-defence-force-munitions [accessed 25 May 2023].

The contract price relates to the 10-year initial contract term and does not include the cost to Defence of additional tenure able to be awarded on the basis of satisfactory contractor performance at the seven-year mark (three years tenure) and nine-year mark (two years tenure).

3 Minister for Defence and Minister for Defence Industry, 'Boosting munitions manufacturing capability in Australia', joint media release, 29 June 2020, available from https://www.minister.defence.gov.au/media-releases/2020-06-29/boosting-munitions-manufacturing-capability-australia [accessed 11 October 2023].

4 For convenience, this report refers to NIOA Munitions/NIOA Nominees Pty Ltd as NIOA. The contract with NIOA commenced on 1 July 2020 and had an original reported value on AusTender of $4.1 million. By 19 June 2024, there had been 22 amendments recorded on AusTender. These amendments related to survey and quote work orders and the reported value had increased to $12.8 million. See https://www.tenders.gov.au [accessed 18 April 2024].

5 Department of Defence, *Defence Strategic Review*, 24 April 2023, available from https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review [accessed 11 October 2023].

do this, the ADF must hold sufficient stocks of GWEO and have the ability to manufacture certain lines, with the realisation of a GWEO enterprise being 'central to achieving this objective.'[6]

5. At 19 June 2024, the implementation of a GWEO enterprise remains a key government priority, with the domestic manufacture of GWEO and munitions in Australia included: as one of seven 'Sovereign Defence Industrial Priorities' in the *Defence Industry Development Strategy* (announced in February 2024)[7]; and as part of the 'immediate priorities' set out in the public versions of the *2024 Integrated Investment Program* (IIP) and the *2024 National Defence Strategy* (both announced on 17 April 2024).[8]

6. On 5 May 2023, the Minister for Defence Industry announced the appointment of a senior responsible officer with responsibility for a Defence GWEO enterprise.[9] At June 2024, Defence's website stated that the facilities at Mulwala and Benalla 'are key assets within the GWEO enterprise and will play a role in the expansion of domestic GWEO manufacturing.'[10]

Rationale for undertaking the audit

7. To establish the arrangements for the operation and maintenance of the Mulwala and Benalla facilities beyond June 2020, Defence undertook a complex and lengthy procurement process that was based on a sole source approach. This audit examined whether this process was effective and in accordance with the *Commonwealth Procurement Rules* (CPRs).

8. This audit builds on previous work by the ANAO which has examined Defence's management of the Benalla and Mulwala facilities over time, and provides independent assurance to the Parliament on Defence's establishment of arrangements for the operation and maintenance of the Mulwala and Benalla facilities beyond June 2020.

Audit objective and criteria

9. The audit objective was to assess whether the arrangements for the operation and maintenance of the Mulwala and Benalla facilities beyond June 2020 were established through appropriate processes and in accordance with the CPRs.

---

6 Department of Defence, *Defence Strategic Review*, 24 April 2023, p. 68.

7 See: Minister for Defence Industry and International Development and the Pacific, 'Landmark strategy to maximise support for Defence industry', media release, 29 February 2024, available from https://www.minister.defence.gov.au/media-releases/2024-02-29/landmark-strategy-maximise-support-defence-industry [accessed 29 February 2024] and Department of Defence, *Defence Industry Development Strategy,* 29 February 2024, pp. 18–19, available from https://www.defence.gov.au/about/strategic-planning/defence-industry-development-strategy [accessed 29 February 2024].

8 See Department of Defence, *Integrated Investment Program,* 17 April 2024, pp. 15–16, available from https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program [accessed 22 April 2024]; Department of Defence, *National Defence Strategy,* 17 April 2024, p. 38, available from https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program [accessed 22 April 2024].

9 Minister for Defence Industry and International Development and the Pacific, 'Moving ahead to manufacture long-range weapons and munitions in Australia', media release, 5 May 2023, available from https://www.minister.defence.gov.au/media-releases/2023-05-05/moving-ahead-manufacture-long-range-weapons-and-munitions-australia [accessed 18 June 2024].

10 See: https://www.defence.gov.au/project/gweo [accessed 4 January 2024].

10. To form a conclusion against the audit objective, the following high-level criteria were selected:

- Did Defence plan effectively for the operation and maintenance of the facilities beyond the expiry of the 2015–20 interim contract?
- Did Defence conduct an effective sole source procurement process to establish the 2020–30 contractual arrangements?
- Did Defence effectively manage probity throughout the process?

11. This report is the first of two performance audit reports examining Defence's establishment and management of the facilities beyond June 2020. It focuses on Defence's establishment of the 2020–30 operating arrangements, including the tender assessment process, advice to decision makers and the decision to conduct a sole source procurement. Defence's management of performance against the contract is the focus of a second report, which will be presented for tabling later in 2024.

Conclusion

12. Defence's conduct of the sole source procurement for the operation and maintenance of the Mulwala and Benalla facilities beyond June 2020 was partly effective. Defence's management of probity was not effective and there was evidence of unethical conduct.

13. Defence's planning processes prior to the expiry of the 2015 interim contract were partly effective. While options for the management of the facilities beyond June 2020 were developed, deficiencies were identified in Defence's subsequent procurement and probity planning processes and in its advice to decision-makers. Defence's decision to conduct a sole sourced procurement was not informed by an estimated value of the procurement prior to this decision and Defence did not document the legal basis for selecting a sole sourced procurement approach, as required by the CPRs. Probity risks were realised in 2016 when Defence personnel provided Thales with confidential information relating to its Investment Committee (IC) proposal, and advice to decision-makers did not address how value for money would be achieved and commercial leverage maintained in the context of a sole source procurement.

14. Defence's conduct of the sole source procurement process to establish the 2020–30 contractual arrangements was partly effective. Risk assessments were not timely and appropriate records for key meetings with Thales during the tender process were not developed or retained by Defence. After assessing Thales' tender response as not being value for money in October 2019, Defence proceeded to contract negotiations in December 2019 notwithstanding internal advice that Defence was at a disadvantage in such negotiations due to timing pressures.

15. The negotiated outcomes were not fully consistent with Defence's objectives and success criteria. Defence's approach to negotiating the contract in accordance with high-level issues reduced the line of sight between the request for tender (RFT) requirements and the negotiated outcomes. Defence's advice to ministers on the tender and contract negotiations did not inform them of the extent of tender non-compliance, basis of the decision to proceed to negotiations, or 'very high risk' nature of the negotiation schedule.

16. Defence did not establish appropriate probity arrangements in a timely manner. A procurement-specific probity framework to manage risks associated with the high level of

interaction between Defence and Thales was not put in place until July 2018. Probity risks arose and were realised during 2016 and 2017, including when a Defence official solicited a bottle of champagne from a Thales representative. Defence did not maintain records relating to probity management and could not demonstrate that required briefings on probity and other legal requirements were delivered.

Supporting findings

Planning during the interim contract period

Options development and consideration of facilities management beyond June 2020

17. Defence provided advice to the Minister for Defence during 2014 on a range of options for the management of the facilities beyond June 2020, including: continuing with the status quo; the Commonwealth operating the facilities; and closing the facilities. These options continued to be considered by Defence and the government between 2015 and mid-2017. In 2016, a clear preference emerged to sole source the operation and maintenance of the facilities to the incumbent, Thales. By July 2016, Defence was primarily focused on developing a proposed 'strategic partnership' arrangement with Thales. Defence did not document the legal basis (that is, an exemption provided by paragraph 2.6 of the CPRs) for the proposed sole source activity to inform its subsequent procurement planning (see paragraphs 2.1 to 2.51).

18. A procurement-specific probity framework was not put in place until July 2018, to help manage probity risks in the context of pursuing a strategic partnership arrangement with Thales. These risks crystallised during 2016 when:

- senior Defence personnel advised Thales at an October 2016 summit meeting that Defence's preference would be to progress a government-owned contractor-operated arrangement with Thales into the future.
- a Defence official sought assistance from and provided information to Thales in November 2016 on the development of internal advice to the IC, Defence's committee processes, and internal Defence thinking and positioning. Government information of this sort is normally considered confidential, and the relevant email exchange evidenced unethical conduct (see paragraphs 2.48 to 2.51).

Advice and analysis informing the decision to conduct a sole source process with the incumbent operator

19. Defence's advice to the IC in December 2016 and the Minister for Defence Industry in mid-2017 on the decision to sole source was not complete. The advice did not address the legal basis for the procurement method, the risks associated with a sole source procurement approach, or value for money issues — including how Defence expected to achieve value for money and maintain commercial leverage in the context of a sole source procurement. When the IC approved the sole source procurement method in December 2016, Defence had not estimated the value of the procurement. This was not consistent with the CPR requirement to estimate the value of a procurement before a decision on the procurement method is made (see paragraphs 2.52 to 2.71).

Establishment of the 2020–30 arrangements

Procurement planning activities

20. Defence's procurement planning activities were not timely. Prior to mid-2017, Defence's planning had largely focussed on seeking approval by June 2017 to inform Thales of the arrangements for the facilities beyond June 2020 (as required of Defence under the interim contract) and to enable collaborative contract development with Thales to commence. Defence's advice to decision-makers was not informed by the results of key planning processes, as required by the CPRs and Defence's procurement policy framework. These key processes were not conducted until after December 2016, when the sole source procurement method was approved and included:

- the progressive development of Defence's requirements for the facilities between March 2017 and July 2019, with assistance from Thales; and
- internal workshops between October 2017 and May 2018, which identified risks that had not been previously documented. Defence did not develop a risk management plan to actively manage those risks (see paragraphs 3.1 to 3.31).

Development of the request for tender

21. Defence undertook a process which included the principal elements of a complex procurement as set out in Defence's procurement policy framework, including an Endorsement to Proceed (EtP), RFT process and detailed contract negotiations. A feature of Defence's process was the high level of interaction with Thales on the contents of the RFT before and after it was issued on 16 August 2019, including during the tender response period. Defence's Complex Procurement Guide (CPG) identified 'probity risks inherent in such activities' and stated that relevant engagement processes and activities 'should be planned and conducted with appropriate specialist support.' Seeking specialist advice on the propriety and defensibility of its approach would have been prudent and consistent with the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) duty that officials exercise care and diligence (see paragraphs 3.32 to 3.63).

Tender evaluation

22. By October 2019, Defence had determined that Thales' tender response was not value for money due to assessing the proposal as 'Deficient – Significant' with 'High' risk against all five evaluation criteria and identifying 199 non-compliances against the RFT. Defence considered the number of non-compliances to be 'unprecedented' and initially agreed, internally, to extend the interim contract with Thales to allow sufficient time to negotiate the non-compliances with the RFT (see paragraphs 3.64 to 3.78).

23. Following senior-level discussions in November 2019 with Thales, Defence decided to conclude the evaluation process on 4 December 2019 and proceed to contract negotiations. This decision was made notwithstanding internal advice that Defence was at a disadvantage in negotiations due to timing pressures. Defence's internal advice considered that it had no 'off-ramps' due to the impending expiry of the interim contract on 30 June 2020. Defence did not clearly document the basis for reducing risk ratings against all the evaluation criteria from 'High' to 'Medium', following the senior-level discussions with Thales (see paragraphs 3.79 to 3.90).

24. Defence did not prepare or retain appropriate records for key meetings with Thales during the tender where the identified risks required active Defence management in the Commonwealth interest. Defence's approach to record keeping was not consistent with requirements in the relevant Communications Plan, internal procurement advice, guidance in the CPG, or the CPRs (see paragraphs 3.91 to 3.100).

Negotiation outcomes

25. The negotiated outcomes for the 2020–30 contract were not fully consistent with Defence's objectives and success criteria approved by Defence in July 2019. At the conclusion of negotiations in February 2020, three of the 15 success criteria aimed at incentivising satisfactory performance and reducing the contract management burden and total cost of ownership for the facilities were reported as not achieved. Defence's approach to negotiations involved agreeing a schedule and high-level negotiation issues with Thales, to guide negotiations between December 2019 and February 2020. Defence did not systematically address the 199 non-compliances it had identified in Thales' tender response. This approach reduced the traceability between the RFT requirements, risks and issues identified during tender assessment, and the negotiated outcomes in the agreed contract (see paragraphs 3.101 to 3.114).

26. Defence's advice to its ministers on the tender and 2020–30 contract negotiations did not inform them of key issues such as the extent of tender non-compliance, the basis of the decision to proceed to negotiations, and Defence's assessment of the 'very high risk' nature of the negotiation schedule (see paragraphs 3.115 to 3.133).

Probity management

Establishment of probity arrangements

27. Defence did not establish appropriate probity arrangements in a timely manner. Defence did not have project and procurement-specific probity arrangements in place until July 2018, more than two years after its initial engagement with Thales (in March 2016) about future domestic munitions manufacturing arrangements. Prior to establishing these probity arrangements, Defence did not assess or take steps to manage potential probity risks arising from ongoing direct engagement with the incumbent operator or remind those involved of their probity obligations, including in relation to offers of gifts and hospitality. During this period, probity risks were realised and there was evidence of unethical conduct, including when a Defence official solicited a bottle of champagne from a Thales representative (see paragraphs 4.1 to 4.30).

28. While Defence's CPG identified 'inherent' probity risks in 'any procurement that involves high levels of tenderer interaction' Defence did not appoint a probity adviser that was external to the department. Defence maintained a register of probity documentation but did not retain relevant records for one of the 65 personnel recorded as having completed documentation. For 22 (25 per cent) of the 87 personnel who completed probity documentation, this completion was not recorded in any register. There was no relevant probity documentation for a further six individuals involved for a period in the procurement. Defence's conflict of interest (COI) register for the procurement was also incomplete. It did not record six instances where a Defence official or contractor declared a potential, perceived or actual COI, including a Tender Evaluation Board member's declaration of long-term social relationships with Thales staff. Defence was unable to

provide evidence that briefings on probity and other legal requirements were delivered in accordance with the Legal Process and Probity Plan for the procurement (see paragraphs 4.31 to 4.50).

Recommendations

Recommendation no. 1
Paragraph 2.31

The Department of Defence document at the time the proposed procurement activities are decided:

- the circumstances and conditions justifying the proposed sole source approach, to inform subsequent procurement planning; and
- which exemption in the CPRs is being relied upon as the basis for the approach and how the procurement would represent value for money in the circumstances.

Department of Defence response: *Agreed.*

Recommendation no. 2
Paragraph 2.61

The Department of Defence, including its relevant governance committees, ensure that when planning procurements, the department estimates the maximum value (including GST) of the proposed contract, including options, extensions, renewals or other mechanisms that may be executed over the life of the contract, before a decision on the procurement method is made.

Department of Defence response: *Agreed.*

Recommendation no. 3
Paragraph 2.64

The Department of Defence, including its relevant governance committees, ensure that advice to decision-makers on complex procurements is informed by timely risk assessment processes that are commensurate with the scale, scope and risk of the relevant procurement.

Department of Defence response: *Agreed.*

Recommendation no. 4
Paragraph 3.61

The Department of Defence ensure that when it undertakes complex procurements with high levels of tenderer interaction, it seeks appropriate specialist advice, including from the Department of Finance as necessary.

Department of Defence response: *Agreed.*

Recommendation no. 5
Paragraph 3.94

The Department of Defence ensure compliance with the Defence Records Management Policy and statutory record keeping requirements over the life of the 2020–30 Strategic Domestic Manufacturing contract, including capturing the rationale for key decisions, maintaining records, and ensuring that records remain accessible over time.

Department of Defence response: *Agreed.*

Recommendation no. 6
Paragraph 3.112

The Department of Defence ensure, for complex procurements, that there is traceability between request for tender (RFT) requirements, the risks and issues identified during the tender assessment process, and the negotiated outcomes.

Department of Defence response: *Agreed.*

Recommendation no. 7
Paragraph 4.10

The Department of Defence develop procurement-specific probity advice for complex procurements at the time that procurement planning begins and develop probity guidance for:

- complex procurements involving high levels of tenderer interaction; and
- managing engagement risks in the context of long-term strategic partnership arrangements.

Department of Defence response: *Agreed.*

Recommendation no. 8
Paragraph 4.25

The Department of Defence make appointment of external probity advisers mandatory for all complex procurements with high probity risks, such as procurements with high levels of tenderer interaction.

Department of Defence response: *Agreed.*

Summary of entity response

29. The proposed audit report was provided to Defence. Defence's summary response is reproduced below. The full response from Defence is at Appendix 1. Improvements observed by the ANAO during the course of this audit are listed in Appendix 2.

Department of Defence

Defence acknowledges the findings contained in the audit report on Defence's Management of Contracts for the Supply of Munitions, which assessed the effectiveness of the procurement and contract establishment for the Department's Strategic Domestic Munitions Manufacturing contracting arrangement.

The Mulwala and Benalla munition factories underpin Australia's ability to develop critical propellants, explosives and munitions for the Australian Defence Force and are recognised as a world-class capability. Since this procurement activity, the strategic landscape has changed, as outlined in the Defence Strategic Update of 2020 and the Defence Strategic Review in 2023. The National Defence Strategy further prioritises these factories as critical and foundational industrial capabilities for Australian domestic manufacturing, supporting sovereign resilience and our allies.

Defence welcomes collaborative engagement with our industry partners in delivering unique capability outcomes. Defence acknowledges and understands the need to ensure that such engagement is appropriately managed, and will strengthen the guidance in relation to identifying and managing procurement and probity risks early in the process as well as maintaining these records for the life of the procurement activity. Defence is continually improving and updating the Defence frameworks that underpin the issues raised.

Key messages from this audit for all Australian Government entities

30. 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.

Procurement

- Entities can demonstrate compliant, transparent, and accountable procurement processes through the creation and retention of appropriate records, including for: decisions on the procurement approach; assessment against selection criteria; engagement with tenderers; and the rationale for proceeding to negotiations.
- Procurements involving high levels of interaction with potential tenderers require active management of engagement probity risks, including ensuring that all relevant interactions are appropriately documented and visibility is maintained over key records such as conflict of interest declarations and probity advice.
- Effective risk management during procurement processes is supported by identifying, assessing and treating procurement risks early in the process and thereafter on an ongoing basis, including developing and maintaining a risk management plan, risk registers, and mitigation strategies for all risks.

The Auditor-General
Auditor-General Report No.45 2023–24
Performance Audit

Defence’s Management of Recruitment Advertising Campaigns

Department of Defence

Australian National Audit Office

Audit snapshot

Auditor-General Report No.45 2023–24

Defence's Management of Recruitment Advertising Campaigns

Why did we do this audit?

- Campaign advertising for Australian Defence Force (ADF) recruitment is an ongoing Department of Defence (Defence) activity and represented about 34 per cent of all Australian Government campaign advertising expenditure in 2022–23.
- Defence has identified 'investing in the growth and retention of a highly skilled workforce to meet Australia's defence and national security requirements' as one of its seven key activities.

Key facts

- The ANAO selected three ADF campaigns which were launched in 2022–23: *Take a Closer Look, Where It All Begins* and *Live a Story Worth Telling*.
- Objectives of the campaigns included increasing the target audience's awareness about a rewarding career in the ADF and inspiring action to find out more or apply.

What did we find?

- Defence's management of the three selected advertising campaigns for ADF recruitment was largely effective.
- For the selected campaigns, Defence complied with most of the review, certification and publication requirements of the campaign advertising framework and largely complied with the requirements of Principles 1 to 4 of the relevant Australian Government Guidelines on Information and Advertising Campaigns.
- Defence monitors the performance of its active campaigns but does not conduct evaluations to determine their effectiveness, as it is required to do.
- There is scope for Defence to improve the transparency of its public reporting on individual advertising campaigns.

What did we recommend?

- There were three recommendations aimed at improving the transparency of Defence's public reporting on individual advertising campaigns and complying with the campaign advertising framework with respect to end of campaign evaluations.
- Defence agreed to all three recommendations.

$60.2 million

amount reported as spent on campaign advertising for Defence Force Recruiting (DFR) in 2022–23 by the Department of Finance.

33.6%

DFR advertising campaign expenditure as percentage of all expenditure reported for Australian non-corporate entities in 2022–23.

22.9%

amount of planned growth in the ADF between 2020–21 and 2042–43.

Summary and recommendations

Background

1. Australian Defence Force (ADF) recruitment advertising campaigns are typically the largest conducted by Australian Government entities each year. The Department of Finance reported that the Department of Defence's (Defence's) recruitment advertising expenditure was $60.2 million for 2022–23, representing approximately 33.6 per cent of total Australian Government advertising expenditure of $179.3 million.[1] In conjunction with a range of contracted suppliers, Defence designs and administers advertising campaigns aimed at particular target audiences.

2. Australian Government entities are required to comply with a framework established by the *Australian Government Guidelines on Information and Advertising Campaigns by non-corporate Commonwealth entities* (the Guidelines).[2]

3. The Guidelines state that they 'operate on the underpinning premise that':

   a. members of the public have equal rights to access comprehensive information about government policies, programs and services which affect their entitlements, rights and obligations; and

   b. governments may legitimately use public funds to explain government policies, programs or services, to inform members of the public of their obligations, rights and entitlements, to encourage informed consideration of issues or to change behaviour.

4. The Guidelines are a government policy and entities subject to them must be able to demonstrate compliance with five overarching principles when planning, developing and implementing publicly-funded information and advertising campaigns. The principles require that campaigns are:

- relevant to government responsibilities;
- presented in an objective, fair and accessible manner;
- objective and not directed at promoting party political interests;
- justified and undertaken in an efficient, effective and relevant manner; and
- compliant with legal requirements and procurement policies and procedures.

Rationale for undertaking the audit

5. Campaign advertising for ADF recruitment is an ongoing Defence activity and represents a material component of all Australian Government campaign advertising. In meeting its outcomes, Defence has identified 'investing in the growth and retention of a highly skilled workforce to meet Australia's defence and national security requirements' as one of its seven key

1 Department of Finance, *Campaign Advertising by Australian Government Departments and Entities Report 2022–23*, p.21. The report is issued annually by the Department of Finance and is available from https://www.finance.gov.au/publications/reports [accessed 4 January 2024].

2 Department of Finance, *Australian Government Guidelines on Information and Advertising Campaigns by non-corporate Commonwealth entities,* December 2022, [Internet] available from https://www.finance.gov.au/government/advertising/australian-government-guidelines-information-and-advertising-campaigns-non-corporate-commonwealth-entities [accessed 17 March 2024].

activities.[3] This audit provides independent assurance to the Parliament on Defence's management of selected ADF recruitment advertising campaigns.

Audit objective and criterion

6. The audit objective was to assess the effectiveness of Defence's management of advertising campaigns for Australian Defence Force recruitment.

7. To form a conclusion against the audit objective, the ANAO adopted the following high-level criterion.

- Were the selected campaigns compliant with the Australian Government's campaign advertising framework?

8. The ANAO selected three campaigns for review, which were launched in 2022–23:

- *Take a Closer Look* — launched on 21 August 2022;
- *Where It All Begins* — launched on 6 February 2023; and
- *Live a Story Worth Telling* — launched on 19 March 2023.

Conclusion

9. The Department of Defence's management of the three selected advertising campaigns for Australian Defence Force recruitment was largely effective.

10. For the selected campaigns, Defence largely complied with the review, certification and publication requirements of the Australian Government's campaign advertising framework and complied with the requirements of Principles 1 to 3 of the Guidelines.

11. Defence largely complied with Principle 4 except that it could not provide the ANAO with supporting evidence to verify the accuracy of cost information for each campaign.

12. With respect to Principle 5, Defence did not clearly document the substantive basis for its advice that there were no legal concerns with respect to the campaign materials.

13. Defence does not evaluate the overall effectiveness of its recruitment advertising campaigns after they have ended. The extent to which Defence's recruitment advertising activities have contributed towards increasing the number of applications to join the ADF has therefore not been assessed by Defence.

14. There is scope for Defence to improve the transparency of its public reporting on individual advertising campaigns and to strengthen the assurance provided to the Secretary of Defence on compliance with the principles of the campaign advertising framework.

Supporting findings

Defence campaigns — compliance with requirements

15. For the three selected campaigns, Defence complied with most of the review, certification and publication requirements of the campaign advertising framework.

3 Department of Defence, *2023–27 Corporate Plan*, August 2023, [Internet] available from https://www.defence.gov.au/about/strategic-planning/defence-corporate-plan [accessed 22 April 2024].

16. Each campaign received government approvals in accordance with the framework requirements applying at the time they were considered. (See paragraphs 2.8 to 2.33)

17. The Defence Secretary completed certifications that the campaigns complied with the five 'overarching principles' of the Guidelines and the certifications were published on Defence's website. The Secretary's certifications were informed by a third-party certification from the Independent Communications Committee (ICC) as required by the Guidelines, and Defence advice on compliance. (See paragraphs 2.12, 2.23 and 2.31)

18. As required by the framework, Defence developed a 2022–23 Media Strategy that was reviewed by the ICC. The ICC provided a report to the Defence Secretary, which was published on the Department of Finance's website as required. (See paragraphs 2.34 to 2.40)

19. Defence did not publish research reports for the selected campaigns on its website and did not document why it was not appropriate to do so. (See paragraphs 2.17, 2.25 and 2.32)

20. While Defence's annual report includes information on overall campaign expenditure, it does not specify the individual advertising campaigns conducted by Defence, as required by the Public Governance, Performance and Accountability Rule 2014 (PGPA Rule). (See paragraphs 2.14, 2.25 and 2.33)

21. Defence complied with the requirements of Principles 1 to 3 of the Guidelines.

22. Defence largely complied with Principle 4 except that it could not provide the ANAO with supporting evidence to verify the accuracy of cost information that it provided. In the absence of this information, no assurance can be provided on the accuracy or completeness of the campaign advertising expenditure as advised by Defence. (See paragraphs 2.102 to 2.107)

23. With respect to Principle 5 (compliance with legal requirements and procurement policies and procedures), Defence did not clearly document the substantive basis for its advice that there were no legal concerns with respect to the campaigns. (See paragraphs 2.72 to 2.75)

24. Defence uses quarterly Communications Tracking reports to monitor the performance of its active campaigns. Defence does not evaluate the overall effectiveness of its recruitment advertising campaigns after they have ended. The extent to which Defence's recruitment advertising activities have contributed towards increasing the number of applications to join the ADF has therefore not been assessed by Defence. (See paragraphs 2.102 to 2.107)

Recommendations

Recommendation no. 1
Paragraph 2.15

The Department of Defence comply with the requirement of the *Public Governance, Performance and Accountability Rule 2014* to include a statement, in its annual report, on the specific advertising campaigns conducted by Defence.

Department of Defence response: *Agreed.*

Recommendation no. 2
Paragraph 2.100

The Department of Defence provide the Department of Finance with details of expenditure on individual Defence advertising campaigns for inclusion in Finance's annual report on *Campaign Advertising by Australian Government Departments and Entities*.

Department of Defence response: *Agreed.*

Recommendation no. 3
Paragraph 2.108

To meet the requirements of the *Australian Government Guidelines on Information and Advertising Campaigns by non-corporate Commonwealth entities* and the *Commonwealth Evaluation Policy*, for future advertising campaigns, the Department of Defence:

(a) establish clear objectives for each campaign prior to the development of the campaign;

(b) document an evaluation plan; and

(c) at the conclusion of each campaign, prepare a final evaluation report.

Department of Defence response: *Agreed.*

Summary of entity response

Department of Defence

Defence acknowledges the Auditor-General's assessment that Defence has mostly complied with the requirements of the Government's advertising framework and related guidelines, and its management of three selected ADF advertising campaigns has been largely effective as a result.

Defence notes that each of its campaigns are subject to rigorous and comprehensive quarterly evaluations over the life of a campaign, a period of typically four to six years, to regularly assess the audience's resonance with, recollection of, and reaction to, the subject campaign. However, Defence accepts the finding that it has not conducted a final evaluation of campaigns it has elected to remove from market.

Defence agrees with the recommendations regarding the improvements to transparency in formal reporting. While Defence has reported expenditure connected to all of its advertising campaigns in annual reports authored by the Department of Defence and the Department of Finance, Defence has not provided details relating to expenditure by campaign, an action it will undertake in formal reporting in the future.

Key messages from this audit for all Australian Government entities

25. 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.

Governance and risk management

- Entities demonstrate transparency and accountability to the Parliament by complying with all annual reporting requirements specified in the *Public Governance, Performance and Accountability Rule 2014*.
- Establishing clear objectives at the outset for projects such as campaign advertising supports the conduct of an effective evaluation process at their completion.

The Auditor-General
Auditor-General Report No.6 2023–24
Performance Audit

Defence Assistance to the Civil Community

Department of Defence

Australian National Audit Office

Audit snapshot

Auditor-General Report No.6 2023–24

Defence Assistance to the Civil Community

Why did we do this audit?

- Defence Assistance to the Civil Community (DACC) provides the means through which the Department of Defence (Defence) can assist other organisations or agencies, often during natural disasters and other emergencies.
- The Australian Defence Force's (ADF's) role in providing such assistance may come at a cost to force preparedness, readiness and combat effectiveness.

Key facts

- DACC support is classed as either 'emergency assistance' (DACC categories 1– 3) or 'non-emergency assistance' (DACC categories 4–6).
- Operation Bushfire Assist 2019–20 involved more than 6500 ADF personnel, including 3000 reservists, making the operation the largest ADF mobilisation for domestic disaster relief in Australian history.

What did we find?

- Defence has established largely effective planning and administrative arrangements to support the provision of emergency DACC.
- The effectiveness of its arrangements is reduced by shortcomings in implementation, monitoring and reporting against requirements.

What did we recommend?

- There were four recommendations to Defence aimed at improving the: recording of costs; cost recovery advice to Ministers; post-activity reporting; and recording of lessons learned.
- Defence agreed to the four recommendations.

748

emergency DACC tasks recorded as completed between 27 May 2013 and 30 June 2022.

$91.5 million

recorded cost of DACC provided under Operation Bushfire Assist 2019–20 and Operation Flood Assist 22–1.

16 days

average duration of emergency DACC tasks under Operation Bushfire Assist 2019–20 and Operation Flood Assist 22-1 and 22-2.

Summary and recommendations

Background

1. Department of Defence (Defence) assistance during emergencies is provided under Defence Assistance to the Civil Community (DACC) arrangements and is governed by Defence policy and procedures.[1]

2. Defence's mission and purpose is to defend Australia and its national interests in order to advance Australia's security and prosperity. Defence is resourced to deliver against this through the following two outcomes, documented in its Portfolio Budget Statements. DACC activities fall under Outcome 1.

- Outcome 1: Defend Australia and its national interests through the conduct of operations and provision of support for the Australian community and civilian authorities in accordance with Government direction.
- Outcome 2: Protect and advance Australia's strategic interests through the provision of strategic policy, the development, delivery and sustainment of military, intelligence and enabling capabilities, and the promotion of regional and global security and stability as directed by Government.

3. The *Defence Assistance to the Civil Community Policy* (DACC Policy) 'describes the agreed approach to providing Defence assistance to the civil community' and outlines ten key principles that are to be applied by Defence personnel when making decisions about the provision of DACC support.[2] It also sets out that:

> Through the 2020 Defence Strategic Update, Government has directed Defence to enhance its support to civil authorities in response to national and regional crises and natural disasters such as pandemics, bushfires, floods or cyclones. Defence is committed to assisting the civil community in both emergency and non-emergency situations. DACC is a mechanism by which Defence achieves this effect. DACC support is not to involve the use, or potential use, of force (including intrusive or coercive acts) by Defence members.[3]

Rationale for undertaking the audit

4. DACC provides the means through which Defence can assist other organisations or agencies. This assistance delivers an outcome or effect at a time when the recipient's own resources are unlikely to be sufficient and/or have been overwhelmed. The Australian Government has observed, in the context of the recent Defence Strategic Review, that the Australian Defence Force's (ADF) role in providing assistance to the civil community following natural disasters comes at a cost to force preparedness, readiness and combat effectiveness.

---

1 DACC is not conducted under any specific Commonwealth legislation.

2 Department of Defence, *Defence Assistance to the Civil Community Policy* [Internet], 31 August 2021, pp. 4–12, available from https://www.defence.gov.au/sites/default/files/2020-12/DACC-Policy.pdf [accessed 31 March 2023].
The ten key principles outlined in the DACC Policy cover: the nature of support provided and the capability of Defence to provide support; approval processes; command and control arrangements; risk management; financial requirements; and preparation for, and implementation of, the provision of support.

3 ibid., paragraph 1.5.

5. This audit has been undertaken to provide independent assurance to the Parliament on the effectiveness of Defence's administrative arrangements to support the provision of emergency assistance to the civil community.

Audit objective and criteria

6. The objective of the audit was to assess the effectiveness of Defence's planning and administrative arrangements to support the provision of emergency DACC.

7. To form a conclusion against the objective, the following high-level criteria were adopted.

- Does Defence prepare effectively to respond to DACC requests?
- Has Defence established fit-for-purpose arrangements to manage DACC delivery?
- Has Defence established arrangements to assess and learn from DACC activity and reviews?

Conclusion

8. Defence has established largely effective planning and administrative arrangements to support the provision of emergency DACC. The effectiveness of its arrangements is reduced by shortcomings in implementation, monitoring and reporting against requirements.

9. In respect to its planning and preparation for emergency DACC activity, Defence has:

- provided clear guidance on its roles and responsibilities;
- undertaken relevant stakeholder engagement, including at the national and sub-national levels;
- taken appropriate steps to prepare its personnel to deliver DACC;
- undertaken relevant and focused information gathering and planning, including in the lead-up to the High Risk Weather Season; and
- provided advice to the Australian Government and reviewers on the impact of DACC on Defence capability.

10. While fit-for-purpose arrangements have been established to coordinate and deliver DACC, Defence's implementation of these arrangements has been partly effective. Shortcomings identified in the implementation of policy requirements include the completion of risk assessments, cost recovery tasks and monitoring and reporting activities.

11. Defence has established fit-for-purpose arrangements to identify lessons learned from DACC activities, and has included relevant requirements in its guidance and directives. Defence has, however, made limited use of these arrangements and has not complied with all requirements. Defence has partly addressed the findings and recommendations of internal and external reviews of DACC arrangements.

Supporting findings

Preparing to respond to DACC requests

12. Clear guidance on Defence's civil assistance role was provided in October 2020, when the August 2020 DACC policy framework was published. Among other things, the framework outlines

the circumstances in which Defence may provide assistance and how those activities are to be requested and coordinated. Prior to its public release, Defence undertook an internal review of the framework to identify learnings from the 2019–20 bushfires and to inform its response to a government request that existing DACC arrangements be reformed so as to take a more proactive stance for responding to significant natural disasters. (See paragraphs 2.2 to 2.16)

13. Defence's *Concept Plan Coalesce* sets out the operational framework to enable detailed planning for the provision of DACC 2 and DACC 3 support. It was last updated in November 2022 and is supported by eight regional Joint Operations Support Staff (JOSS) support plans, seven of which are to be reviewed annually. At June 2023, four of these plans remained overdue for review by up to 53 months (4.4 years). (See paragraphs 2.17 to 2.21)

14. Since 2020, Defence's engagement with stakeholders has been focused on annual planning and communication activities in preparation for the High Risk Weather Season (HRWS). Defence inputs to the 2022–23 HRWS Preparedness Program included a briefing for each state and territory outlining the process for requesting DACC support, as well as details on Defence's capabilities, HRWS posture, and resource limitations. Defence also drafted a HRWS Communication Plan in December 2020 to identify target audiences, key stakeholders, and the sensitivities and risks for communication around DACC activities. (See paragraphs 2.22 to 2.30)

15. Defence records do not support regular attendance at relevant committees and forums, as required by the DACC Manual since August 2020. At the national level, these include the Australian Government Crisis and Recovery Committee and National Coordination Mechanism. (See paragraphs 2.27 to 2.28)

16. While Defence relies on the DACC Manual and Policy as the primary mechanisms for conveying how DACC is conducted and managed, Defence has also developed awareness raising information for ADF personnel involved in delivering DACC support. For ADF personnel assigned to certain DACC 2 and DACC 3 tasks, e-learning modules and briefings have been developed to cover situational awareness, survivability, expected values and behaviours, guidance on dealing with members of the public and the media, legal considerations, and medical guidance. (See paragraphs 2.31 to 2.36)

17. Defence planning for the delivery of DACC support is largely focused on annual preparations for the HRWS. Chief of the Defence Force (CDF) warning orders and Chief of Joint Operations (CJOPS) task orders for the HRWS over the past three years have outlined Defence's force posture and which of its assets were likely to be required. Defence's planning and advice to decision-makers is informed by the Bureau of Meteorology's Global Seasonal Outlook. (See paragraphs 2.37 to 2.39)

18. Defence has conducted and participated in table-top exercises simulating natural disaster scenarios for flooding, bushfires and cyclones, and for the call-out of Defence reserves. Through its review work, Defence has identified that it does not have a good awareness of reservist civilian qualifications. While the Minister for Defence was advised in June 2020 that qualifications would be captured, tracked and utilised, work to progress the collection of these details remained paused as at March 2023. Defence advised the ANAO in July 2023 that this work would not proceed. (See paragraphs 2.40 to 2.45)

19. While a number of Army Lessons Boards and Fleet Lessons Boards were conducted in 2021 and 2022 to identify areas for improvement after the HRWS, Defence was unable to provide the ANAO with documentation for any Defence-level or Air Force lessons boards. Further, Defence's recording and monitoring of lessons with enterprise-wide implications on its centralised lessons database, the Defence Lessons Repository, has been limited. (See paragraphs 2.46 to 2.50)

20. Since 2020, Defence has provided the Australian Government and reviewers with advice regarding its assessment of the impact of DACC on Defence capability. The risks advised by Defence, which were acknowledged in the Australian Government's response to the 2022 Defence Strategic Review, relate to force preparedness, readiness and combat effectiveness. Defence also advised the Defence Minister that amendments to the *Defence Act 1903* could address legal risks associated with the delivery of DACC support by ADF members, Defence personnel and foreign forces. (See paragraphs 2.51 to 2.64)

Managing the delivery of DACC

21. Defence has long-standing and fit-for-purpose arrangements to coordinate and provide emergency DACC support. These include Joint Task Force (JTF) arrangements that can be activated by the Chief of the Defence Force (CDF) or relevant approving authority, for commanding domestic operations such as responses to natural disasters. To facilitate DACC support, Defence also: establishes an Emergency Support Force each year in each state and territory in anticipation of requests for assistance during the High Risk Weather Season (HRWS); and provides ADF Liaison Officers within state and territory emergency management agencies to assist in the coordination of DACC support. (See paragraphs 3.3 to 3.11)

22. Shortcomings in the application of policy requirements were identified across each of the seven case studies reviewed by the ANAO. Defence did not consistently comply with the DACC Manual in the following respects.

- The initiation and approval requirements for two DACC tasks. In one case Defence sought to avoid triggering the requirement, in the Secretary's Accountable Authority Instructions, to obtain the Defence Minister's approval to waive the recovery of DACC costs. This approach raises both compliance and ethical issues regarding Defence's management of public resources.
- Estimating the costs for five DACC tasks or recording the actual costs associated with the DACC support provided by Defence.
- WHS and risk management requirements — while high-level risk assessments were conducted at the Joint Task Force and Joint Task Group levels, Defence could not demonstrate that risk assessments required at the DACC task-level had been completed. (See paragraphs 3.12 to 3.59)

23. Defence has not consistently applied the cost recovery requirements outlined in the DACC Manual and Defence's Cost Recovery Policy. While Defence has sought Ministerial approval for cost recovery waivers for some DACC 3 tasks, advice to the Minister outlining the reasons for those waivers has not always been consistent with the intent of those policies. (See paragraphs 3.34 to 3.44)

24. Defence personnel do not consistently report on DACC activities as required, weakening Defence's capacity to monitor DACC delivery. Further, information held in the DACC database is

unreliable, in large part because key details of DACC tasks have been recorded incorrectly, or not recorded at all. ANAO review indicates the following.

- The completion of post-activity reports (PARs) has been limited, with 744 (99.5 per cent) of the 748 DACC 1–3 tasks identified as completed since 2013–14 not having a PAR lodgement date recorded.
- For the seven DACC tasks selected for detailed review by the ANAO, situation reporting and PARs had been completed for five of the tasks (71 per cent). For three of these five tasks, the situation reports were either provided late or not provided to all required recipients in accordance with DACC Manual requirements. (See paragraphs 3.60 to 3.89)

25. Between June 2014 and December 2022, the DACC Manual required the preparation of a biannual or annual report for the Chief of the Defence Force (CDF) and Defence Secretary on the level of DACC support provided. This reporting relied on task-level data submitted through PARs. While this reporting was intended to improve compliance with PAR requirements, it last took place in December 2015 and was removed from the DACC Manual released in December 2022. Defence continues to provide other types of reporting to CDF and the Defence Minister, however the current reporting regime does not include task-level information. (See paragraphs 3.90 to 3.99)

Assessing and learning from DACC activity

26. Defence has established fit-for-purpose arrangements to identify lessons learned from DACC activities and has included relevant requirements in the DACC Manual and a joint lessons directive issued by the Chief of Joint Operations (CJOPS). However, it has made limited use of the arrangements and has not complied with all requirements.

27. The Defence Lessons Program (DLP) and Defence Lessons Handbook provide policy, guidance and support for lessons management in Defence. A Defence Lessons Repository (DLR) has also been established for collating observations, insights and lessons (OILs) from Defence activities. However, Defence's limited use of the DLR for DACC purposes does not align with the requirements of the DACC Manual or CJOPS Joint Lessons Directive 48/2022.

28. In the context of 2828 individual tasks recorded in the DACC database as delivered between 27 May 2013 and 30 June 2022, the Defence Lessons Repository included 185 observations, 20 insights and one lesson related to DACC activities recorded since 2013–14. (See paragraphs 4.2 to 4.23)

29. Defence has partly addressed the findings and recommendations of internal and external reviews of DACC arrangements.

- In October 2021 Defence closed out the ten recommendations of an internal review requested by the Australian Government following Operation Bushfire Assist 2019–20. At the time of closure, updates against four of the recommendations noted that implementation activity was still underway. Work relating to a recommendation to track reservist civilian skillsets was subsequently discontinued by Defence.
- An agreed Auditor-General recommendation to review DACC reporting requirements and improve compliance was partly implemented. Defence conducted a review of the DACC Manual in 2014 to consider the minimum reporting requirements necessary to discharge

Defence accountability and transparency obligations. However, the steps taken to strengthen the priority afforded by Defence units to meeting reporting requirements — through the introduction of biannual and later annual reporting to CDF and the Defence Secretary — were short-lived. The last instance of such reporting was in 2015 and the requirement was removed in 2022.

- Defence implemented the three recommendations relating to DACC made in the report of the 2020 Royal Commission into National Natural Disaster Arrangements. (See paragraphs 4.24 to 4.41)

Recommendations

Recommendation no. 1
Paragraph 3.41

The Department of Defence implement arrangements to ensure that costs associated with providing DACC support are accurately tracked and recorded, in line with the requirements of the DACC Manual.

Department of Defence response: *Agreed.*

Recommendation no. 2
Paragraph 3.43

The Department of Defence ensure that its advice to the Minister for Defence in respect to waiving cost recovery for DACC 3 tasks is: aligned with Australian Government and Defence cost recovery policies; appropriately addresses the efficient and effective use of Commonwealth resources; and outlines the financial and resource impacts associated with not recovering costs.

Department of Defence response: *Agreed.*

Recommendation no. 3
Paragraph 3.95

The Department of Defence improve its administrative arrangements for DACC to ensure that:

(a) post-activity reports are completed with all relevant information and submitted according to the requirements of the DACC Manual;

(b) data entered into the DACC database is complete and accurate, and supports reporting to the Chief of the Defence Force (CDF), Secretary of Defence and Minister for Defence; and

(c) the CDF, Secretary and Minister are provided with sufficient and appropriate information on the aggregated costs of DACC support.

Department of Defence response: *Agreed.*

Recommendation no. 4
Paragraph 4.21

The Department of Defence implement arrangements to ensure that relevant observations, insights and lessons identified through post-operation and post-activity DACC reporting are recorded on the Defence Lessons Repository in accordance with Defence policies.

Department of Defence response: *Agreed.*

Summary of Department of Defence's response

30. Defence's summary response is provided below and its full response is included at Appendix 1.

> Defence acknowledges the ANAO's assessment that Defence has established largely effective planning and administrative arrangements to support the provision of emergency Defence Assistance to the Civil Community (DACC).
>
> The focus of the report on the administrative processes provides Defence the opportunity to ensure that policies and practices are refined to optimise support for emergency DACC operations.
>
> The outcomes and implication of the ANAO report will be a key consideration in the next review of the DACC Manual and associated policies.

31. The improvements observed by the ANAO during the course of the audit are at Appendix 2.

Key messages from this audit for all Australian Government entities

32. 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.

Governance and risk management

- Program reviews involve the investment of public resources. Adequate and timely implementation of agreed recommendations helps realise the full benefit of review activity and demonstrates commitment to improved public administration and accountability for performance.

Policy/program implementation

- High-quality policy and guidance documentation supports program implementation and compliance with requirements. Periodic review of documentation helps maintain its fitness-for-purpose.

Performance and impact measurement

- Well-operating lessons learned arrangements can enhance implementation effectiveness, entity efficiency, and review activity. Embedding such arrangements is an investment in effective delivery.
- Project closure activities and effective record-keeping position entities to provide soundly-based information and advice to decision-makers and the Parliament on the impact and outcomes of entity activities.