

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

# **Defence's Procurement and Implementation of the myClearance System**

Department of Defence

© Commonwealth of Australia 2024

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-957-9 (Print)

ISBN 978-1-76033-958-6 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *Australian honours system* website at <https://www.pmc.gov.au/honours-and-symbols/australian-honours-system>.

Requests and inquiries concerning reproduction and rights should be addressed to:

Chief Operating Officer  
Corporate Management Group  
Australian National Audit Office  
GPO Box 707  
Canberra ACT 2601

Or via email:

[communication@anao.gov.au](mailto:communication@anao.gov.au)



Canberra ACT

11 July 2024

Dear President  
Dear Mr Speaker

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

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

Yours sincerely



Rona Mellor PSM  
Acting Auditor-General

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

## **AUDITING FOR AUSTRALIA**

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

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

**Phone: (02) 6203 7300**  
**Email: [ag1@anao.gov.au](mailto:ag1@anao.gov.au)**

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

### **Audit team**

Joyce Knight  
Shane Madden  
Finn Coverdale  
Jude Lynch  
Corne Labuschagne  
Tex Turner  
Olivia Robbins  
Ketan Doshi  
Amy Willmott

# Contents

---

Summary and recommendations.....	7
Background .....	7
Conclusion .....	9
Supporting findings.....	10
Recommendations.....	12
Summary of the Department of Defence’s response .....	12
Key messages from this audit for all Australian Government entities .....	13
<b>Audit findings.....</b>	<b>15</b>
1. Background .....	16
Introduction.....	16
Administrative arrangements.....	20
Previous ANAO reports .....	23
Rationale for undertaking the audit .....	23
Audit approach .....	24
2. Planning and decision-making .....	25
Did Defence conduct effective planning activities? .....	25
Did Defence establish effective governance, oversight and reporting arrangements?.....	45
3. Procurement and implementation .....	61
Did Defence conduct effective procurement processes?.....	62
Did Defence effectively manage implementation? .....	76
<b>Appendices .....</b>	<b>97</b>
Appendix 1     Department of Defence response .....	98
Appendix 2     Improvements observed by the ANAO .....	99
Appendix 3     Vetting Transformation Project budget .....	100
Appendix 4     Vetting Transformation Project — Business Outcomes .....	102
Appendix 5     Functional and non-functional requirements of the future vetting capability .....	104
Appendix 6     Project approval and support services contract with Deloitte — Contract Change Proposals (2017 to 2021).....	106



# 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.



#### 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.



#### 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 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.<sup>1</sup> 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.<sup>2</sup>
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.<sup>3</sup>

## 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.<sup>4</sup>

## 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.<sup>5</sup>
- 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.<sup>6</sup>

## 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.<sup>7</sup>

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**    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.  
**Paragraph 2.53**

**Department of Defence response:** *Agreed.*

**Recommendation no. 2**    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.  
**Paragraph 3.101**

**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.



# Audit findings

# 1. Background

---

## Introduction

1.1 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.<sup>8</sup> 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.

1.2 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.<sup>9</sup>

1.3 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.<sup>10</sup>

## Vetting Transformation Project

1.4 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.

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

---

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

9 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.

10 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.<sup>11</sup>

### First pass approval

1.6 The Australian Government provided first pass approval in April 2018 for the Vetting Transformation Project, with the future vetting solution to be delivered across three modules:

- a core vetting system (the base capability) to replace the existing vetting systems and processes;
- improvements to integrate additional data checks into the vetting capability; and
- integration of a wider range of data checks and provision of an automated continuous assessment functionality.

1.7 At first pass, the government was advised that the estimated whole of life costs for the project were \$276.3 million (\$154.6 million for acquisition and capability development and \$121.7 million for sustainment) over a period of 20 years.<sup>12</sup> This cost was over three times more than the IIP provision of \$68.6 million available for the Vetting Transformation Project.

1.8 To address the shortfall, Defence recommended that the Case Management and Vetting Transformation projects be delivered 'programmatically' (with a joint governance structure) to enable efficient management of the acquisition spend for both projects. The total provision for the two projects at August 2017 is detailed in Table 1.1.

---

11 Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security*, paragraph 2.62.

12 The value of the estimated cost for the Vetting Transformation Project was the same as the IIP provision of \$276.3 million for the Case Management System Project.

**Table 1.1: Capital funding provision for Case Management System Project and Vetting Transformation Project (\$ million), at August 2017**

Project	2017–18	2018–19	2019–20	2020–21	2021–22	2022–23	2023–24	Subtotal	Contingency	Total
Vetting Transformation	9.9	23.8	21.5	0.0	0.0	0.0	0.0	55.3	13.3	68.6
Case Management System	4.2	9.5	23.6	25.2	24.8	51.8	64.4	203.5	72.8	276.3
<b>Total provision</b>	<b>14.1</b>	<b>33.3</b>	<b>45.1</b>	<b>25.2</b>	<b>24.8</b>	<b>51.8</b>	<b>64.4</b>	<b>258.8</b>	<b>86.1</b>	<b>344.9</b>

Source: ANAO analysis of Defence documentation.

### *Revised approach*

1.9 Defence's Investment Committee considered both projects in December 2019. The committee did not support the projects progressing to second pass consideration by government in March 2020 (as planned) as the updated total cost estimate of \$488 million for the projects (developed after first pass) exceeded the available IIP provision by \$144 million. The Investment Committee directed the Chief Information Officer (CIO) to come back in February 2020 with advice on the work required to achieve government consideration by October 2020 of a mature proposal for both projects.

1.10 Between January and April 2020, Defence examined: decoupling the two projects; delivering them as part of Defence's Enterprise Resource Planning (ERP) Program<sup>13</sup>; either or in addition to implementing a simplified technical solution for the Vetting Transformation Project to address the affordability issues. In April 2020, the funds allocated to the two projects were amended under the Force Structure Plan, resulting in the IIP provision for the Vetting Transformation Project increasing from \$68.6 million to \$279.2 million.

1.11 In June 2020, Defence recommended, and the Minister for Defence agreed, to a revised approach for the delivery of the two projects. Vetting Transformation was to be managed as a separate project and the Case Management System project was to be delivered as part of the ERP Program.

### **Second pass approval and project budget**

1.12 In December 2020, the government provided second pass approval of \$307.2 million — comprising \$138.6 million for acquisition (including \$14.7 million contingency) and \$168.6 million for sustainment — over 10 years for the Vetting Transformation Project. It was also agreed that the project would be delivered in two modules, rather than the three proposed at first pass.<sup>14</sup>

1.13 The two modules and expected delivery timeframes are as follows.

- Module one (Core Vetting System) — to replace AGSVA's existing ICT system and manual business processes, improve AGSVA's ability to meet future clearance demands and better detect personnel security risks through automated sharing of risk information.
  - To be delivered by Quarter 4 2022, representing achievement of Initial Operating Capability (IOC).
- Module two (Continuous Assessment for AGSVA managed clearances) — enhance existing and integrate additional data feeds, increase the frequency of checks, and use artificial intelligence to identify and assess security risks in near-real time.
  - To be delivered by Quarter 4 2023, representing achievement of Final Operating Capability (FOC).

---

13 The ERP Program involves streamlining Defence business processes associated with hundreds of separate Defence ICT applications into one SAP S/4HANA system, with the intent of enabling better governance, faster processing and lower maintenance and support costs. Functional areas where applications and processes are in scope for the program are: finance; human resources; supply; maintenance; engineering; procurement and estate. Defence's management of Tranche 1 was reviewed in Auditor-General Report No.1 2021–22 *Defence's Administration of Enabling Services — Enterprise Resource Planning Program: Tranche 1*.

14 The first two modules approved at first pass — comprising the core capability and additional data checks — were consolidated into module one at second pass.

1.14 The Vetting Transformation Project came to be known as myClearance in June 2022.

1.15 The new myClearance system ‘went live’ on 28 November 2022 with the introduction of the base capability. By February 2023, the extent of user issues experienced after the system went live were the subject of parliamentary interest. In November 2023, Defence advised the government that:

- \$120.4 million (87 per cent) of the project’s total acquisition budget (\$138.6 million) had been expended by the end of 2022–23;
- Defence expected to use the entire funding provision, inclusive of the \$14.7 million contingency, to deliver a reduced scope; and
- the cost risk associated with the project had been realised — with the full scope of the project unable to be delivered within the budget approved by government at second pass in December 2020.

1.16 The acquisition and sustainment budget for the project is detailed at Appendix 3.

## Administrative arrangements

1.17 The Defence Digital Group (DDG), previously the Chief Information Officer Group (CIOG)<sup>15</sup> and the Security and Estate Group (SEG) within Defence are jointly responsible for the delivery of myClearance (the Vetting Transformation Project).

- DDG is responsible for contract administration and the technical and architectural aspects of the ICT system.
- SEG is the Project Sponsor, accountable to the Capability Manager (the Associate Secretary), and responsible for managing business process redesign and policy adjustment with oversight provided by the AGSVA Governance Board.

1.18 AGSVA was established in 2010 and is responsible for administering personnel security vetting and the granting and/or denying of security clearances on behalf of the Australian Government.<sup>16</sup> It is part of Defence and sits within the SEG. The Assistant Secretary, Vetting (SES Band 1) is responsible for AGSVA’s day-to-day management. The AGSVA Governance Board provides strategic direction and oversight of AGSVA and monitors the progress of service delivery business reform and systems development.<sup>17</sup> The AGSVA Board is responsible for: setting the

---

15 The DDG was established in mid-2023. The group’s title was CIOG for the majority of the period examined by this audit. For consistency, the group has been referred to only as CIOG throughout this report.

16 Five intelligence and law enforcement agencies are exempt from using AGSVA to grant/deny security clearances to employees and contractors.

17 The AGSVA board has been chaired by the Deputy Secretary, Security and Estate Group since December 2022. Prior to this, the Associate Secretary for Defence was the chair. The board includes representatives from the Australian Public Service Commission (APSC), Australian Security and Intelligence Organisation, Australian Signals Directorate, Department of Finance, Department of Home Affairs, Department of Human Services, Department of the Prime Minister & Cabinet (PM&C), Attorney-General’s Department and the Office of National Intelligence. It met on a quarterly basis between December 2016 and January 2024. Before the project received internal Defence approval to commence in April 2017 (at Gate 0), the board had received two updates on the project.

AGSVA Service Level Charter; setting priorities for the processing of security clearance assessments; reviewing and setting fees; and reports annually to the Secretaries Board.<sup>18</sup>

## Operating context

1.19 Defence's website states that under the Australian Government Protective Security Policy Framework (PSPF), individuals who need access to security classified resources must hold a security clearance. An individual may also be required to hold a security clearance if they occupy a position of trust that requires additional assurance. The purpose of security vetting is to determine whether an individual is suitable to hold a security clearance, that is, whether they possess and demonstrate an appropriate level of integrity. In the security context, integrity is defined as a range of character traits (honesty, trustworthiness, maturity, tolerance, resilience and loyalty) that indicate the individual is able to protect Australian Government classified resources. The security vetting of an individual establishes confidence that they possess a sound and stable character, and they are not unduly vulnerable to influence or coercion.<sup>19</sup>

1.20 Over the period examined by this audit (June 2016 to May 2024), AGSVA processed 452,369 security clearances — an average of 56,546 vetting decisions each year.<sup>20</sup> Out of the 452,369 security clearances processed, AGSVA granted 452,204 (99.96 per cent) and denied 165 (0.04 per cent). The majority (83 per cent) of the decisions to grant a security clearance were at the Baseline and NV1 clearance levels.<sup>21</sup> The number of Baseline, NV1, NV2 and PV clearances processed by AGSVA to May 2024 is illustrated in Figure 1.1 and Table 1.2.

18 Section 64 of the *Public Service Act 1999* establishes the Secretaries Board. The Secretaries Board is chaired by the Secretary of PM&C. Its membership comprises: the secretaries of all Australian Government departments; the Secretary for Public Sector Reform; and the Australian Public Service Commissioner (as Deputy Chair). See: [www.pmc.gov.au/about-us/accountability-and-reporting/corporate-reporting/secretaries-board](http://www.pmc.gov.au/about-us/accountability-and-reporting/corporate-reporting/secretaries-board) [accessed 18 May 2024].

19 AGSVA, 'Security clearance definitions' [Internet], available at: <https://www.agsva.gov.au/about/security-clearance-definitions> [accessed 24 March 2024].

20 A security clearance that has been processed is one where AGSVA has made a decision to either grant or and/or deny the clearance. Figure 1.1 excludes clearance requests that have been cancelled or withdrawn.

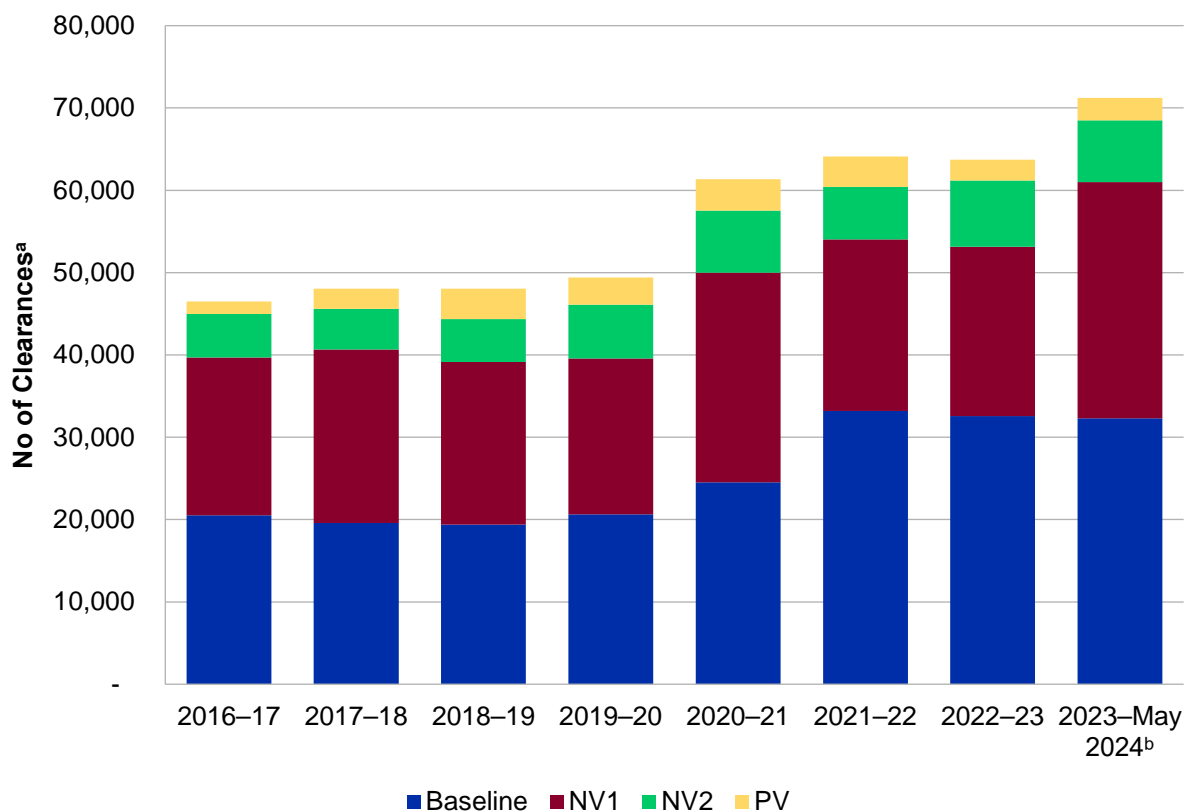
21 There are four levels of security clearances:

- Baseline – permits ongoing access to classified resources up to and including Protected;
- Negative Vetting 1 – permits ongoing access to classified resources up to and including Secret, and temporary access to Top Secret classified resources in certain circumstances;
- Negative Vetting 2 – permits ongoing access to classified resources up to and including Top Secret;
- Positive Vetting – permits ongoing access to classified resources up to and including Top Secret, including some caveated resources.

See: AGSVA, 'Security clearance definitions' [Internet], available at:

<https://www.agsva.gov.au/about/security-clearance-definitions> [accessed 24 March 2024].

**Figure 1.1: Security clearances processed by AGSVA — June 2016 to May 2024**



Note a: The total number of security clearances processed are the clearances that have been granted and/or denied by AGSVA. For the 2023–24 period, AGSVA had processed 71,218 clearances as at 9 May 2024.

Note b: As at 9 May 2024, 107,249 clearances had been processed in the myClearance system since it ‘went live’ on 28 November 2022.

Source: ANAO analysis.

**Table 1.2: Security clearances processed by AGSVA — June 2016 to May 2024**

Clearance level	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22	2022-23	2023-May 2024 <sup>a</sup>
Baseline	20,505	19,577	19,377	20,645	24,532	33,205	32,562	32,300
NV1	19,201	21,065	19,772	18,938	25,451	20,845	20,579	28,688
NV2	5,265	4,955	5,209	6,515	7,569	6,359	8,033	7,495
PV	1,504	2,448	3,683	3,324	3,788	3,690	2,555	2,735

Note a: As at 9 May 2024, 107,249 clearances had been processed in the myClearance system since it ‘went live’ on 28 November 2022.

Source: ANAO analysis.

1.21 In 2022–23, AGSVA processed 63,729 security clearances. For 2023–24, as at 9 May 2024, AGSVA had processed 71,218 security clearances for over 780 government (federal, state and territory) bodies and industry entities.<sup>22</sup>

## Previous ANAO reports

1.22 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.<sup>23</sup>
- 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 the Australian Government’s 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.<sup>24</sup>

## Rationale for undertaking the audit

1.23 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.<sup>25</sup>

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

22 Industry entities include companies that are members of the Defence Industry Security Program and non-government agencies whose employees are contracted to provide services for, or on behalf of, a government agency.

23 Auditor-General Report No.45 2014–15, *Central Administration of Security Vetting*, para 13.

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

25 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].

## Audit approach

### Audit objective, criteria and scope

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

1.26 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)?

1.27 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 service providers.

### Audit methodology

1.28 The audit methodology involved:

- examining records related to planning, governance, procurement and implementation of the Vetting Transformation Project (the myClearance system); and
- meetings with relevant Defence personnel and personnel contracted by Defence to deliver the Vetting Transformation Project (the myClearance system).

1.29 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately \$932,000.

1.30 The team members for this audit were Joyce Knight, Shane Madden, Finn Coverdale, Jude Lynch, Corne Labuschagne, Tex Turner, Olivia Robbins, Ketan Doshi and Amy Willmott.



## 2. Planning and decision-making

### Areas examined

This chapter examines the effectiveness of the Department of Defence's (Defence) planning activities for the Vetting Transformation Project (myClearance) and the effectiveness of the governance, oversight and reporting arrangements.

### Conclusion

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.

### Recommendations

The ANAO made one recommendation aimed at improving Defence's risk management for complex and high value ICT projects.

2.1 Effective planning processes and oversight arrangements support entity compliance with the *Public Governance, Performance and Accountability Act 2013* (the PGPA Act) and are fundamental for sound project management. In the context of complex procurements and ICT projects, effective governance, oversight and reporting arrangements should ensure that decision-makers are well-informed of project progress and the potential impact of emerging risks.

### Did Defence conduct effective planning activities?

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.

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.

## Capability Life Cycle framework

2.2 Defence commenced planning in late 2016 for the Vetting Transformation Project, which was among the first information and communications technology (ICT) projects to be delivered under Defence's newly established Capability Life Cycle framework. The Capability Life Cycle was introduced by Defence as a central part of the 'One Defence' model following the 2015 First Principles Review.<sup>26</sup> Defence defines the Capability Life Cycle as the process of introduction, sustainment, upgrade and replacement of Defence capability.<sup>27</sup> It is a 'core business process in Defence which is critical in enabling Defence to perform its primary role of defending Australia and its national interests'.<sup>28</sup>

2.3 Defence's Capability Life Cycle framework encompasses all major expenditure decisions taken by Defence, including major military equipment, ICT, facilities, workforce and other service delivery functions. Under the framework, the responsibility for capability delivery is split between the Capability Manager, the subordinate Program and/or Project Sponsor (the 'customer') and the Delivery Lead (the 'supplier'). The Project Sponsor for the Vetting Transformation Project was the Australian Government Security Vetting Agency (AGSVA) within the Security and Estate Group and the Delivery Lead was the Chief Information Officer Group (CIOG).<sup>29</sup>

2.4 The Capability Life Cycle comprises four phases: 'Strategy and Concepts', 'Risk Mitigation and Requirement Setting', 'Acquisition', and 'In Service [or sustainment] and Disposal'.

2.5 As illustrated by Figure 2.1, the risk mitigation and requirement setting phase for the Vetting Transformation Project was over twice the duration of the acquisition (or implementation) phase. Delays in Defence's procurement processes to engage the systems integrator (see paragraphs 3.39 to 3.44) were a large contributing factor in the protracted planning period.

2.6 To manage the division of responsibilities, the 2016 Capability Life Cycle Manual (that was in effect at the time) identified a suite of agreements and plans (governance documents) to be developed at the portfolio, program and project/product levels.<sup>30</sup> The five 'key governance documents' that were

26 Defence's early implementation of the One Defence model was examined as part of Auditor-General Report No.34 2017–18 *Defence's Implementation of the First Principles Review*, paragraph 4.4.

27 Defence's Capability Life Cycle Manual states that a 'capability' is:  
generated by combining equipment, workforce, organisation, estate, logistics and other systems. In Defence, the standard list of these inputs is known as the Fundamental Inputs to Capability. An important objective of planning is to ensure that all of these inputs are delivered in the quantities, characteristics and timescales to generate and sustain the capability, combined in an optimum way to deliver a joint [Defence] force by design.

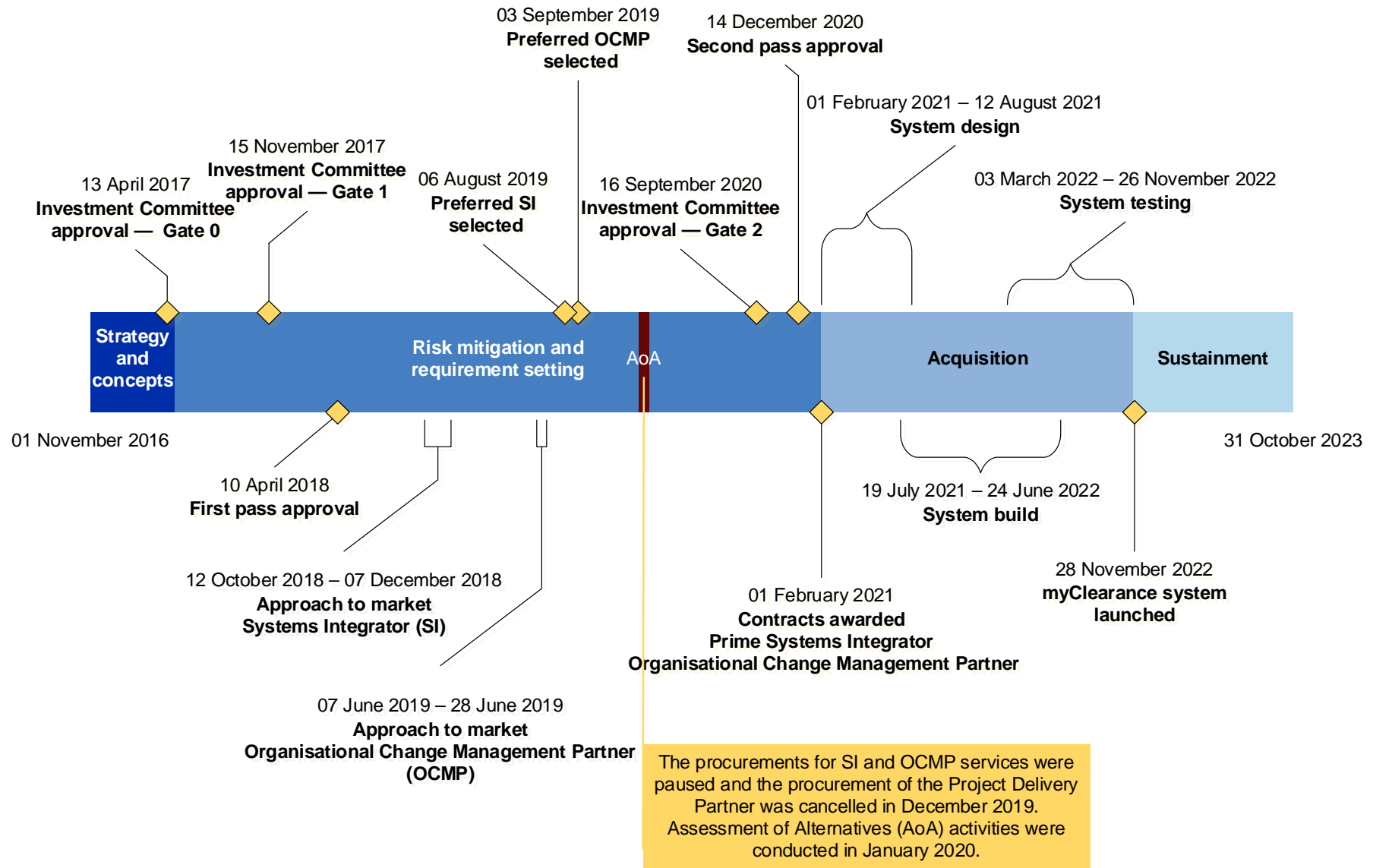
28 Defence's early implementation of the One Defence model was examined as part of Auditor-General Report No.34 2017–18 *Defence's Implementation of the First Principles Review*, paragraph 4.4.

29 As part of an internal Defence restructure, CIOG was replaced by the Defence Digital Group (DDG) in mid-2023. As the group's title was CIOG for majority of the period examined by this audit it has been referred to as CIOG throughout this report.

30 The portfolio level applies to the management of all approved and unapproved capability proposals in the Integrated Investment Program (IIP). The program level applies to a group of related projects and/or products to deliver a common capability effect, and the project level applies to a single initiative to deliver a specific capability requirement or meet an identified business need.




to be produced and refined for the Vetting Transformation Project during the first two phases of the Capability Life Cycle (December 2016 to December 2020) are examined in Table 2.1.



**Figure 2.1: Key milestones for the Vetting Transformation Project across the four phases of Defence's Capability Life Cycle**



Source: ANAO analysis of Defence documentation.

**Table 2.1: Key governance documents for the Vetting Transformation Project, as required by Defence’s Capability Life Cycle Manual**

Document	To be developed and finalised by (including revision dates where required)		Description	ANAO analysis	
Program Strategy <sup>a</sup>	The Program Sponsor (AGSVA) on behalf of the Capability Manager (Associate Secretary)	April 2017 (Gate 0)	Articulates the Capability Manager’s plan to achieve capability outcomes across a group of products and projects, including the transition planning for capabilities.	A Program Strategy was not developed for the Vetting Transformation Project, as part of a broader program of activities, until November 2020.  In November 2020, the project was identified as part of the Defence Business Enterprise Architecture Transformation (DBEAT) Program. <sup>d</sup>	
Project Directive	VCDF as Chair of the Defence Investment Committee	April 2017 (Gate 0)	Constitutes the formal approval issued by the Vice Chief of the Defence Force (VCDF) after the Investment Committee decision or after approval has been issued by government. The Project Directive reflects the approved scope and timeframes for the next sequence of activities, the responsibilities and resources allocated and the key risks and issues.	A Project Directive was not issued as required (by Defence’s Capability Life Cycle framework) following approval from the Defence Investment Committee in April 2017 (Gate 0), to enable the project to progress to the Risk Mitigation and Requirement Setting phase.	
Product Delivery Agreement <sup>b</sup>	CIOG as the Delivery Lead	September 2020 (Gate 2)	Project and Product specific delivery agreement between the Project Sponsor, Integrated Project/Product Manager and the Fundamental Inputs to Capability <sup>c</sup> representatives.  It provides the metric-focused baselines for performance reporting, in order to support the consolidation and aggregation of performance data at a program and portfolio level.	A Product Delivery Agreement, referred to as the Materiel Acquisition Agreement (MAA) between AGSVA and CIOG, was developed in December 2020. It was not implemented or maintained as required.	

Document	To be developed and finalised by (including revision dates where required)	Description	ANAO analysis
Project Execution Strategy <sup>b</sup>	CIOG as the Delivery Lead April 2017 (Gate 0) November 2017 (Gate 1) September 2020 (Gate 2)	A high level, risk-based tailored strategy to support the Investment Committee's decision-making for a project or proposal. The project execution strategy consists of four strategies, developed using the Smart Buyer Decision Making Framework, in order to articulate the intended project approval pathway and project management, acquisition and sustainment activities.	The Project Execution Strategy was initially developed in March 2017 and further refined throughout the Risk Mitigation and Requirement Setting phase (April 2017 to September 2020). 
Integrated Project Management Plan (IPMP) <sup>b</sup>	CIOG as the Delivery Lead November 2017 (Gate 1) September 2020 (Gate 2)	A plan to manage the delivery of a project and coordinate the Fundamental Inputs to Capability. The IPMP describes the detailed conduct of activities to sustain a Product and deliver a Project.	An IPMP was initially developed in August 2017 and further refined between May 2019 and October 2020. 

Key:  Met requirements  Partially met requirements  Did not meet requirements.

Note a: A program strategy was required as the Vetting Transformation Project was part of a broader ICT program (a group of five projects) intended to transform business processes across Defence.

Note b: The Delivery Lead (CIOG) engaged an external service provider for project approval and support services (Deloitte). These services included the development of these key project governance documents.

Note c: The 2016 Capability Life Cycle Manual defined Fundamental Inputs to Capability (FIC) as inputs that are to be combined and integrated to successfully introduce and/or achieve the desired capability uplift. There were nine FIC: organisation; command and management; personnel; collective training; major systems; facilities and training areas; supplies; support; and industry.

Note d: The DBEAT Program included the following projects: Enterprise Information Management (EIM), Case Management System (CMS), and Vetting Transformation and the Enterprise Resource Planning (ERP) Program. The DBEAT Program has been referred to as the Defence Business Integration Program (DBIP) since July 2022. Defence established DBIP in July 2022 to oversee the implementation of large-scale business transformation projects. In November 2023, Defence advised government that the program was in an early stage of maturity and the projects under the DBIP had independent schedules and implementation activities.

Source: ANAO analysis of Defence documentation.

## Market research and industry engagement

2.7 Defence's April 2017 Complex Procurement Guide (that was in effect at the time) stated that having sound knowledge of the market is a key enabler of good procurement outcomes. It also stated that Defence officials should conduct market research and obtain market intelligence commensurate with the value and complexity of the procurement. In March 2017, Defence advised its Investment Committee that for the Vetting Transformation Project:

Market research will be undertaken to establish a clear understanding of the capability available, including the availability of COTS [commercial-off-the-shelf] solutions. If a viable COTS solution is not available across the market locally or internationally, further engagement with industry will be undertaken. The project will look to leverage the key findings and lessons learned from other mature vetting solution implementations, available in the market and examples across other defence forces and agencies. The availability of COTS solutions will need to be validated based on further requirements definition.

2.8 These market research and industry engagement activities were conducted by an external service provider (Deloitte) and informed the development of three key planning documents Deloitte was tasked with preparing.<sup>31</sup> These documents were the Joint Capability Needs Statement, Business Case and Project Execution Strategy. Each of these documents addressed aspects of Defence's approach to industry engagement.

2.9 The market research identified two vetting projects that delivered capabilities similar to those required by Defence. One was delivered in the United States of America (USA) in 2013 and the other in the United Kingdom (UK) in 2016. The market intelligence report noted that neither project had delivered the full capability proposed by the Vetting Transformation Project (see paragraphs 2.18 to 2.19).

- The UK's 'National Security Vetting Solution' delivered workflow management, task co-ordination, online application, status monitoring and process automation.
- The USA's 'Automated Continuous Evaluation System' (ACES) included automated data feeds from other entities and ongoing candidate suitability assessments.

2.10 Between July and December 2017, Deloitte developed an initial overview (environmental scan) of the market to identify the technologies and products available and the providers with the capabilities needed to deliver the project. The scan found that there was a range of 'commercial off the shelf' (COTS) products available across the four categories of technology required: vetting technologies<sup>32</sup>; continuous assessment technologies<sup>33</sup>; data services<sup>34</sup>; and other required

---

31 Deloitte was engaged in November 2016 to provide Project Approval and Support services and develop and deliver the artefacts necessary to achieve Investment Committee approval.

32 The vetting technologies were comprised of 12 components: a web content management system; interactive voice recognition; vetting portal; vetting management system; vetting model and risk/rules management; reporting and analytics; financial management; identity and access management; information and record management; enterprise service bus; integration gateway; and database services.

33 The continuous assessment technologies were comprised of five components: vetting model and risk rules management; artificial intelligence and machine learning; continuous risk assessment; decision support; and data aggregation.

34 The data services identified included information from social media and financial credit check specialists.

services.<sup>35</sup> It also noted that while there was a broad range of products available, they needed to be successfully integrated to provide the end-to-end vetting solution required.

### **Development of the future vetting model and capability requirements**

2.11 Effective consultation during the planning phase for complex ICT systems (such as the Vetting Transformation Project), enables future user requirements to be fully defined and used to inform the design and development of the new system.

2.12 Defence assessed the 'business need' and developed the 'capability requirements' for the new system in accordance with its Capability Life Cycle Manual. This work was iterative and was led by Deloitte throughout the first two phases of the Capability Life Cycle — the 'Strategy and Concepts' and the 'Risk Mitigation and Requirement Setting' phases.

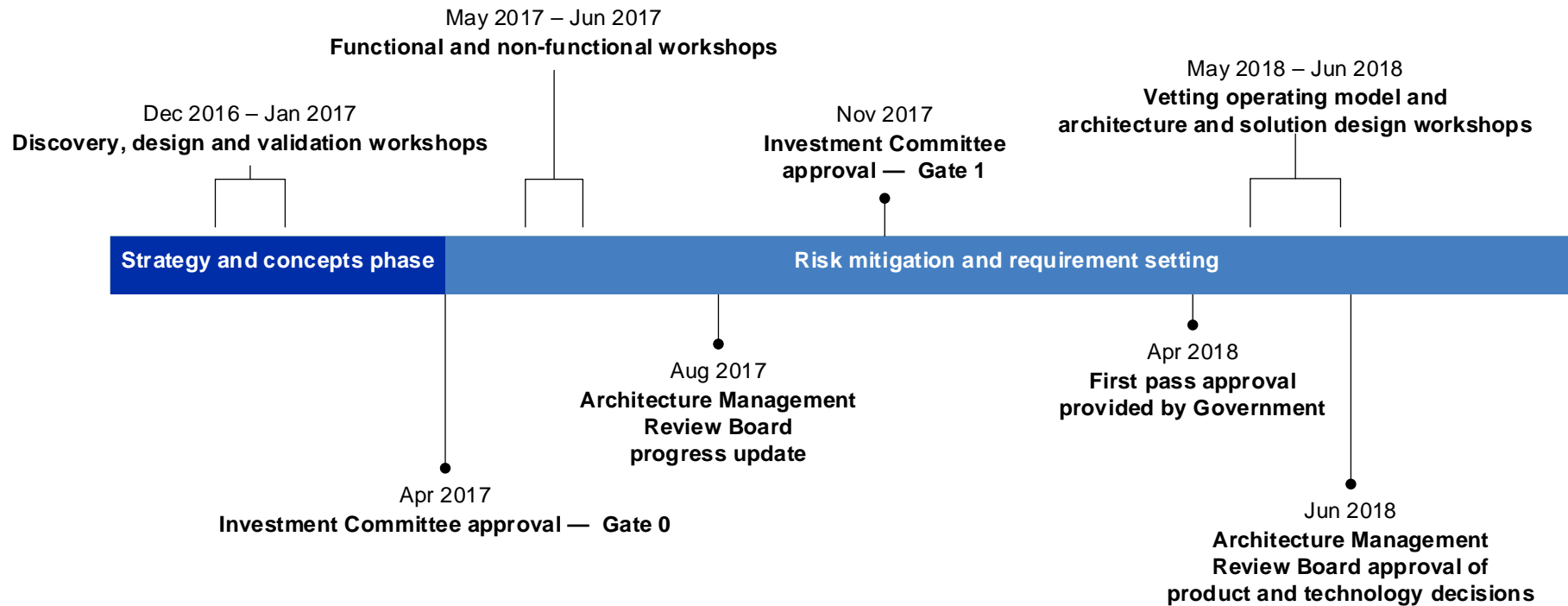
2.13 The key project milestones across these two phases are illustrated in Figure 2.2.

---

35 Other required services to successfully deliver the Vetting Transformation Project included Systems Integrators and Intellectual Property (IP) providers.



**Figure 2.2: Key milestones and planning activities for the Vetting Transformation Project during the first two phases of the Capability Life Cycle**



Source: ANAO analysis of Defence documentation.

### *Planning workshops and internal approvals*

2.14 Two series of workshops were conducted prior to Gate 1 approval in November 2017, and a further series was conducted between May and June 2018 after first pass approval had been provided by government.

2.15 Results from the ‘discovery, design and validation’ workshops (conducted in December 2016 and January 2017<sup>36</sup>) informed the development of the Business Case, Joint Capability Needs Statement, and the Project Execution Strategy. These documents were presented to Defence’s Investment Committee in April 2017 as part of the Gate 0 approval process.<sup>37</sup> At Gate 0, the Investment Committee approved the use of a two-pass approval process for the project and noted the need for Defence to ‘consider and clearly outline the commonalities across other ICT projects being considered by the Committee’.<sup>38</sup>

2.16 After Gate 0 approval in April 2017, Defence commenced work to further develop and refine the future vetting operating model and the capability (functional and non-functional) requirements of the replacement ICT system. As part of developing the operating model, Defence identified the stakeholders, organisations, roles, products, services, processes and policies involved in the personnel security vetting process.<sup>39</sup> Figure 2.3 provides an overview of the results of this activity.

---

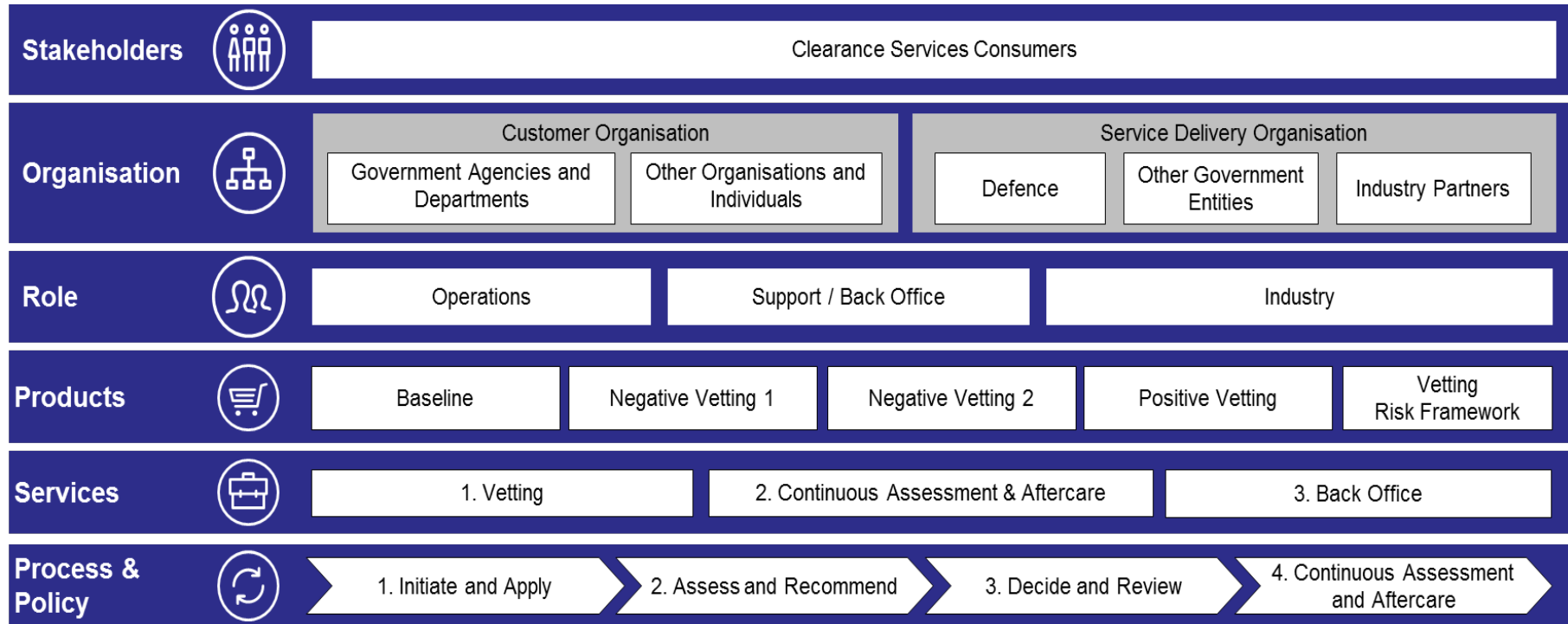
36 Six workshops were held with 132 representatives invited to participate. Of the 88 participants, 14 (16 per cent) were from other government departments and industry, and 74 (84 per cent) were from Defence.

37 Gate 0 approval constitutes formal approval to commence a project and marks the completion of the strategy and concepts phase of the Capability Life Cycle.

38 The related/linked ‘inflight’ projects were those delivering an application or technology that the Vetting Transformation Project would need to leverage, be compatible with, integrate or interface with.

39 Defence identified 167 potential policies relevant to the future vetting capability and refined the list down to 26 policies with which the future vetting operating model would need to comply.

**Figure 2.3: Scope of the business considerations to develop the future vetting operating model**



Source: Extract from Defence records — Vetting Transformation Gate 1 — Vetting Transformation Process and Conceptual Architecture.

2.17 The functional and non-functional requirements of the replacement ICT system were further developed and refined across seven workshops held between 24 May and 21 June 2017. The requirements were informed by interviews with stakeholders, reviews of the existing vetting system, and business process mapping. A total of 160 representatives participated in the workshops, with 132 (82 per cent) from Defence, 27 (17 per cent) from other government entities, and one (one per cent) from industry.<sup>40</sup>

2.18 By July 2017, Defence had confirmed that the replacement ICT system should include a core vetting system and continuous assessment functionality. The core vetting system was to comprise: a web content management system; a vetting portal ('System of Engagement'<sup>41</sup>) to replace the ePack<sup>42</sup> and related dashboards; a vetting management system ('System of Record') and vetting model; and risk rules management to replace PSAMS2.<sup>43</sup>

2.19 In response to the Investment Committee's April 2017 request that commonalities across other ICT projects be considered (see paragraph 2.15), Defence advised the committee in November 2017 that the new vetting system would do the following.

- Use the same technology and licences as the Case Management System Project.<sup>44</sup>
- Be compatible with the content management, information and records management, and improved analytics and reporting frameworks, being developed by the Enterprise Information Management Project.
- Use the identity services being delivered by the Identity and Access Management Project for Defence users, with external users to utilise trusted third-party identity brokers.
- Access data from the financial management module being delivered by the Enterprise Resource Planning (ERP) Program.
- Access human resource management information being delivered by the Defence One Project.

Gate 1 approval

2.20 The Investment Committee provided Gate 1 approval on 15 November 2017. This gave the project authority to: select realistic options for further development; agree the risk appetite, tolerance and treatment plan; agree the proposed scope, budget and schedule; and formally engage with industry (approach the market). Defence's plan to approach the market for a systems integrator is discussed in more detail in paragraphs 2.33 to 2.39.

2.21 Twelve workshops were facilitated by Defence's Project Approval and Support Services Provider (Deloitte) over six weeks between 8 May 2018 and 14 June 2018. The purpose of the

---

40 The industry representative was an external vetting services provider from the industry vetting panel.

41 Defence defined the System of Engagement as a system that provides a common user interface across agreed existing and future Defence systems.

42 The ePack was an electronic form sent to clearance subjects for completion at the commencement of a security vetting process. Once completed, the security vetting pack was submitted through an online portal.

43 The Personnel Security Assessment Management System (PSAMS2) was the case management system used by AGSVA before myClearance went live in November 2022.

44 In June 2017, the Case Management System project identified that it intended to implement SAP Investigative Case Management as part of a SAP ecosystem solution, where SAP Investigative Case Management would be the system of record for complex case types and MS Dynamics as the system of record for simple case types, with one or more systems of engagement.

workshops was to refine the future vetting operating model and the business processes for each phase of the future security vetting process, see Figure 2.4. A range of external stakeholders involved in sponsoring and/or processing security clearances were to contribute to these design discussions to assist with the identification of all user requirements.<sup>45</sup>

**Figure 2.4: Future state end to end security clearance vetting process**



Source: ANAO representation of Defence's Vetting Operating Model at Gate 2 approval.

2.22 External stakeholders were to be invited to participate in three of the 12 workshops between May and June 2018. There are no attendance records to demonstrate that external service providers, security officers or other government entities attended these sessions.<sup>46</sup>

2.23 An 'Architecture and Solution Design Working Group' was established in May 2018 to refine the technical components of the core vetting module and continuous assessment functionality of the vetting system. The working group was comprised of project personnel from Defence and the contracted project approval and support services provider (Deloitte). Membership of the working group did not include other stakeholders or systems owners, such as other government entities with ICT systems required to interface with AGSVA's system.<sup>47</sup>

2.24 On 29 June 2018, Defence's Architecture Management Review Board endorsed the product guidance and directions proposed by the Architecture and Solution Design Working Group. In August 2018, Defence held a market pre-brief session where prospective suppliers were provided an overview of the technology components required to deliver the core vetting module and continuous assessment functionality of a future vetting solution. In October 2018, the request for quotation (RFQ) was released. The approach to market, and the impact of the product guidance and directions included in the RFQ, are examined at paragraphs 2.33 to 2.39.

Gate 2 approval

2.25 In September 2020, the operating model, and solution design and technical architecture were finalised and presented to the Defence Investment Committee for Gate 2 approval and endorsement to seek second pass approval from government.

2.26 Defence advised the Investment Committee that it had identified 12 business outcomes for the Vetting Transformation Project (see Appendix 4), six categories of functional requirements and

45 These stakeholders included other government entities, external vetting service providers (such as those contracted to AGSVA), psychologists (engaged to screen and assess the character and eligibility of clearance subjects to hold a security clearance), and agency security officers and industry sponsors (officers with responsibility for monitoring personnel risks and the ongoing eligibility of staff to hold a clearance on behalf of their respective organisations).

46 One attendee external to Defence (a contracted psychologist) was present at one of the operating model sessions.

47 In April 2024, Defence advised the ANAO that the Architecture and Design Working Group had consulted with representatives from other government departments to refine various technical components, including the external integrations and interfaces with systems owned and operated by other government departments.

eight categories of non-functional requirements (see Appendix 5). The Investment Committee was also advised that the future vetting capability would meet the following business needs:

- increased efficiency of vetting to reduce processing timeframes for all clearance levels;
- increased use of data from trusted Government and non-Government sources to inform vetting decisions and clearance subject risk profiles;
- scalability to account for future demand and growing workforce from sponsoring entities;
- flexibility to adapt, for example to emerging threats and changes in policy;
- seamless transfer of information to other government agencies in order to perform security assessment functions;
- improved analysis and sharing of risk information with sponsoring entities, enabling more effective management of personnel security threats through advanced analytics and continuous evaluation;
- improved user experience, including updates on the progress of security clearance applications;
- reduced risk to loss of information due to the means of accessing and corroborating data from other Government agencies; and
- secure system access for industry service providers, negating the need to transport paper files between Defence and industry.

## Options development and refinement

2.27 Defence initially identified six options to deliver the future vetting capability. Each option was assessed against the following six criteria: strategic alignment, functional fit, technical fit, cost, change requirements, and implementation complexity. Three options were set aside and three progressed to more detailed analysis in August 2017. Table 2.2 outlines the options that were progressed.<sup>48</sup>

**Table 2.2: Shortlisted options to deliver the future vetting capability**

Option	Description	Delivers	Estimated cost
1. Improved vetting service and continuous assessment (full solution)	<ul style="list-style-type: none"> <li>• Delivery of improved vetting services, including: replacing PSAMS2, ePack(s), the Security Officer Dashboard and numerous manual processes.</li> <li>• Implements a full continuous assessment solution.</li> </ul>	<ul style="list-style-type: none"> <li>• Improved vetting services.</li> <li>• Analytics and reporting.</li> <li>• Continuous assessment and clearance maintenance processes and systems.</li> </ul>	\$156 m

<sup>48</sup> The options set aside were: 'Do Minimal', 'Do Nothing (base case)' and 'Fully Outsourced Vetting Function'.

Option	Description	Delivers	Estimated cost
2. Improved vetting service and continuous assessment, Positive Vetting (PV) only	<ul style="list-style-type: none"> <li>• Delivery of improved vetting services, including: replacing PSAMS2, ePack(s), the Security Officer Dashboard and numerous manual processes.</li> <li>• Implements a scalable continuous assessment solution with initial data integrations for PV clearance subjects only.</li> </ul>	<ul style="list-style-type: none"> <li>• Improved vetting services.</li> <li>• Improved analytics and reporting.</li> <li>• Scalable continuous assessment solution.</li> </ul>	\$118 m
3. Improved vetting service	<ul style="list-style-type: none"> <li>• Delivery of improved vetting services, including: replacing PSAMS2, ePack(s), the Security Officer Dashboard and numerous manual processes, including key integrations.</li> </ul>	<ul style="list-style-type: none"> <li>• Improved vetting services.</li> <li>• Improved analytics and reporting.</li> <li>• Improved existing revalidation process.</li> </ul>	\$68 m

Source: ANAO analysis of Defence documentation.

2.28 Option one (the full solution) was presented to Defence’s Investment Committee as the preferred option in November 2017 for Gate 1 approval. Defence noted that all three options could be delivered incrementally, with options two and three considered interim solutions in the lead up to delivery of the full solution. The Investment Committee approved proposing to government that the full solution be delivered using a ‘modular approach to implementation’.

2.29 The government agreed in April 2018 to Defence’s recommendation that the full solution be delivered through the following three modules.

- Module one (improved vetting service): would deliver the core vetting system by replacing the existing vetting systems and business processes.
- Module two (improved vetting service and continuous assessment for holders of PV clearances only): would make improvements to the core vetting system, integrate additional data checks, and provide continuous assessment functionality for a subset of clearance holders.
- Module three (improved vetting service and continuous assessment): would integrate a wide range of data checks and apply continuous assessment functionality to all security clearance holders, except for holders of a baseline clearance.

### Procurement planning for a systems integrator

2.30 Defence commenced planning work in August 2017 to procure the services needed to design, build, test and deploy the new ICT solution. Key to this was the engagement of a systems integrator. The Business Case submitted to the Defence Investment Committee in November 2017 advised that up to \$156.3 million would be required to deliver the capability — \$87.7 million greater than the IIP provision of \$68.6 million over 20 years.<sup>49</sup> Costs for the systems integration services were estimated at \$82.6 million (53 per cent of the total funding estimate).

<sup>49</sup> See Table 1.1. The \$68.6 million approved IIP provision for the Vetting Transformation Project was comprised of \$55.3 million and \$13.3 million contingency.

2.31 Several ‘stages of analysis’ were conducted to compile a ‘suitable candidates list’ by July 2018 for the procurement of the systems integrator. These analyses included the following.

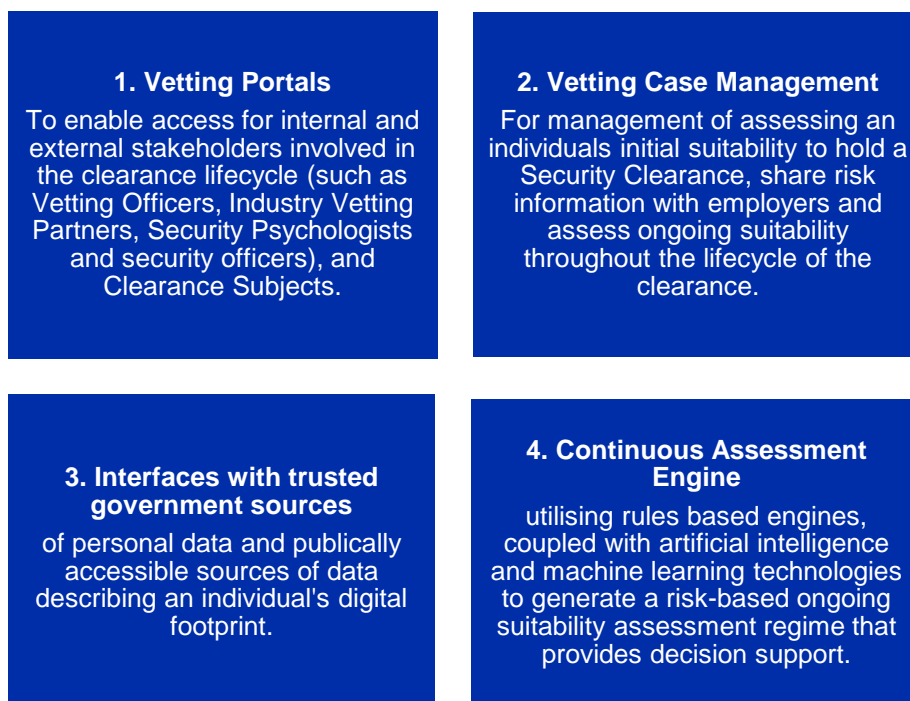
- Market analysis conducted by Deloitte in February 2018 for the Case Management Project and in March 2018 for Vetting Transformation. Eleven potential suppliers were identified.
- Following the establishment of the new Information and Communications Technology Provider Arrangement (ICTPA) panel in July 2018, ‘high level desktop research was performed’ on suppliers on the panel that had not been identified through the market analysis.

2.32 Of the 23 suppliers on the ICTPA panel that ‘qualified for systems integrator and application development services’, 16 were selected as potential candidates for the procurement. These 16 included five suppliers that had been identified through the earlier market analysis.<sup>50</sup>

*Approach to market*

2.33 Potential suppliers, identified through the processes discussed at paragraph 2.31, were invited to attend a market pre-brief session in August 2018. Eleven suppliers attended and were informed that Defence was seeking to transform its existing vetting services, processes and technologies. The prospective suppliers were also advised that the project was linked to the Case Management Systems Project, was part of a broader Enterprise Business Transformation Program and was to deliver the broad capability functions illustrated in Figure 2.5.

**Figure 2.5: Capability functions to be delivered through the Vetting Transformation Project**



Source: ANAO representation of extract from Defence records — Market Pre-Brief, 15 August 2018.

<sup>50</sup> The other six suppliers identified through the analysis were not invited to respond to the RFQ as they were considered ‘not eligible ... as they are not on [the] ICTPA’ panel. Defence’s ICTPA panel requirements are discussed further in paragraphs 3.16 to 3.23.



2.34 On 12 October 2018, Defence issued a request for quote (RFQ), for systems integration and application development services, to 15 prospective suppliers selected from the ICTPA panel.<sup>51</sup> An industry briefing session was held on 23 October 2018. The required technology, associated architecture and applications discussed at the briefing were set out across five components — four ‘Technology Components’ and one ‘Continuous Assessment Component’. The RFQ and industry briefing also included a range of ‘guidance’ to potential suppliers for each component of the RFQ, including the following mandatory specifications.

- One or more of eight specified ‘Candidate Products’ as the ‘System(s) of Engagement’ (SOE, or Vetting Portal).<sup>52</sup>
- SAP Investigative Case Management (SAP ICM) as the ‘System of Record’ (SOR, or Vetting Platform).
- For the ‘Vetting Model and Risk Rules Management’, ‘Continuous Assessment’ and ‘Other Supporting Technologies’ components, suppliers were to either:
  - adopt ‘the products currently deployed by Defence to deliver the capability’; or
  - propose goods and technology solutions available from Defence or whole-of-government panels or existing Defence or Commonwealth agreements.

2.35 As discussed at paragraph 2.45, Defence expected these requirements to enable cost efficiencies and reduce the technical risk of the project.<sup>53</sup> These mandatory specifications placed constraints on potential suppliers and discouraged the development of alternative solutions. This approach was inconsistent with Defence’s procurement policy framework, and the intent of the CPRs. Defence’s Complex Procurement Guide (March 2018), which applied at the time, stated that:

Even if a procurement is not subject to Division 2 of the CPRs, the rules should be followed as good practice. In particular the CPRs require that technical specifications ... be set out in terms of functional and performance requirements, rather than, for example, as specific design or descriptive characteristics (because this would lead to the specification of particular products themselves rather than specifications that products would be required to meet).

2.36 The 2018 CPRs, which were in effect at the time, stated that:

A *specification must* not require or refer to a particular trademark or trade name, patent, copyright, design or type, specific origin, producer, or *supplier*, unless there is no other sufficiently precise or intelligible way of describing the requirement. In an exceptional circumstance when this type of *specification* is used, words such as ‘or equivalent’ **must** be included in the *specification* [emphasis in original].<sup>54</sup>

2.37 Defence’s RFQ did not contain wording to this effect. Rather, suppliers were advised that alternative proposals would be accepted only for the SOE, and alternatives would only be evaluated, if the supplier had already lodged a quotation that met the mandatory specifications. Suppliers were

51 IBM was not invited. At the time, IBM had been engaged as the systems integrator for Defence’s ERP Project.

52 These products were: Appian; BPM Online; Microsoft Dynamics; Oracle Unified Business Process Management Suite; OpenText Process Suite; Pegasystems Pega; SAP products including SAP FIORI; and ServiceNow.

53 In April 2024, Defence advised the ANAO that ‘Defence made an enterprise architecture decision to make SAP the single System of Record across Defence’.

54 Department of Finance, *Commonwealth Procurement Rules*, 1 January 2018, paragraph 10.12, [internet] available from <https://www.finance.gov.au/government/procurement/commonwealth-procurement-rules> [accessed 14 March 2023].

also advised that proposals must use SAP Investigative Case Management as part of a SAP Ecosystem solution ‘as it is the Defence directed SOR for [the Vetting Transformation Project]’.

2.38 Potential suppliers were to specify the goods required for their proposed solution in a costed ‘Bill of Materials’. The rationale provided for this in the RFQ was that the ‘provision of goods is out of scope for this RFQ, will be procured separately by Defence, and provided to the supplier as Government Furnished Materials (GFM) under the Work Order’.

2.39 Defence’s procurement process for the systems integrator is examined further in paragraphs 3.3 to 3.55.

## Risk identification

2.40 A new risk profiling tool was implemented by Defence in October 2016 as part of its Smart Buyer Decision Making Framework. The tool outlined 17 risk categories — nine for acquisition and eight for sustainment — that were ‘likely to be common to many, if not all Defence projects and programs’. Defence used this approach to develop the risk profile outlined in the Project Execution Strategy for the Vetting Transformation Project.<sup>55</sup>

2.41 The initial risk profile was presented to Defence’s Investment Committee on 13 April 2017. Due to the ‘high’ and ‘medium-high’ risk ratings allocated to six (66 per cent) of the nine acquisition stage risks, the acquisition risk profile of the project was initially assessed as ‘high’.

2.42 The risk profile was reassessed during the Capability Life Cycle. The results of these assessments are set out in Table 2.3.

**Table 2.3: Vetting Transformation Project risk profile**

Risk category	Apr 2017 <sup>a</sup>	Jul 2017	Nov 2017 <sup>b</sup>	Jun 2018	Sep 2020
	Gate 0	Smart Buyer Workshop No.1	Gate 1	Smart Buyer Workshop No.2	Gate 2
Acquisition					
Requirements	High	Medium–low	Medium–low	Medium–low	Medium–low
Defence Integration	High	Medium–high	Medium–high	Medium–low	Medium–low
Schedule	High	High	High	Medium–high	Medium–high
Project Integration	Medium–high	Medium–high	Medium–high	Medium–low	Medium–low
Technology	Medium–high	Medium–high	Medium–high	Medium–low	Medium–low
Strategic	Medium–high	Low	Low	Medium–high	Medium–low

55 The Defence Procurement Policy Manual set out the various risk categories to be considered when developing the Project Execution Strategy (PES). Development of a PES is a requirement of Defence’s capability development framework and is used, among other things, to inform the Defence Investment Committee’s consideration of complex procurements.

Risk category	Apr 2017 <sup>a</sup>	Jul 2017	Nov 2017 <sup>b</sup>	Jun 2018	Sep 2020
Financial	Medium–low	High	High	Medium–low	Medium–low
Commercial	Medium–low	Medium–low	Medium–low	Medium–low	Medium–low
Industry Capability	Low	Medium–low	Medium–low	Medium–low	Medium–low
Sustainment					
In-Service Requirements	Medium–high	Medium–high	Medium–high	Medium–high	Medium–low
Obsolescence	Medium–high	Medium–high	Medium–high	Medium–high	Medium–low
FIC	Medium–high	Medium–low	Medium–low	Medium–high	Medium–low
Commercial	Medium–low	Low	Low	Medium–high	Medium–low
Financial	Medium–low	High	High	Medium–low	Medium–low
Strategic	Low	Low	Low	Medium–low	Medium–low
Operational	Low	Low	Low	Low	Low
Industry Capability	Low	Medium–low	Medium–low	Medium–low	Medium–low

Note a: The risk profile presented to Defence's Investment Committee in April 2017 was developed as part of the Gate 1 approval process and to seek first pass government approval.

Note b: The risk profile presented to Defence's Investment Committee in November 2017 was developed as part of the Gate 2 approval process and to seek second pass government approval.

Source: ANAO analysis of Defence documentation.

### *Review of identified risks*

2.43 Between July 2017 and September 2020, Defence reassessed the risks and updated the risk profiles outlined in the Project Execution Strategies presented to the Investment Committee in November 2017 (at Gate 1) and September 2020 (at Gate 2). The activities to reduce the risk ratings for the integration, schedule, technology, and financial categories are examined below in paragraphs 2.44 to 2.50.

#### Integration risks

2.44 There were two integration risk categories: project integration and Defence integration. The project integration risk category relates to the volume, complexity and criticality of the interfaces between the system hosted in the Defence ICT environment and its links to other ICT environments. For example, the interfaces with the Australian Criminal Intelligence Commission (ACIC) to run police checks on clearance subjects and the interface with the Australian Security Intelligence Organisation (ASIO) to transfer cases for security assessments. The Defence integration risk relates to the complexity of integrating the new system into the Defence ICT environment.

2.45 To reduce the project integration risk rating from 'medium-high' to 'medium-low', Defence advised its Investment Committee in November 2017 that it would prioritise the implementation of external data integrations based on criticality and ease of implementation. To reduce the Defence integration risk from 'high' to 'medium-low', Defence directed the market to use SAP ICM for the System of Record (see paragraph 2.34). The intention was to reduce the risk and the number and

complexity of internal integrations by using the same technology as the Case Management System Project (see paragraph 2.19). As discussed at paragraph 2.35, this approach introduced a critical dependency, increased the schedule risk and was not in line with Defence policy or the CPRs.

#### Schedule risks

2.46 The schedule risk category relates to the extent of flexibility in the delivery schedule. In April 2017, Defence noted that the risk would be mitigated by the Integrated Project Team and the oversight provided by the governance arrangements. Defence advised the Investment Committee in November 2017 that the risk rating remained 'high' and this was largely due to dependencies on other Defence projects and the lead time required to successfully migrate critical data. Defence identified that the risk would be managed by:

- testing the ability of the market to adopt an iterative approach to deliver the capability, with initial 'capability drops' commencing as early as 2020; and
- continuing to manage the schedule, dependencies and risks through the project management processes and governance arrangements established.

2.47 Defence reassessed the schedule risk in June 2018 and downgraded it from 'high' to 'medium-high'. Nevertheless, Defence noted that the schedule to deliver the Final Operating Capability was 'aggressive'. The 'medium-high' rating remained unchanged in September 2020 (at Gate 2), with Defence advising its Investment Committee that IOC would be delivered by Quarter 4 2022 and FOC by Quarter 4 2023.

#### Technology risks

2.48 To reduce the technology risk assessment from 'medium-high' to 'medium-low' Defence completed a technical risk indicator report in December 2017. The assessment identified that the technical risk was low, due to Defence's intention to use COTS components for the future vetting solution and integrate them into the Defence ICT environment. It was noted that this presented a substantial amount of integration complexity. In June 2019, the technical risk was again assessed as low, noting that these risks were associated with the systems integration and continuous assessment capabilities to be delivered in the future.

#### Financial risks

2.49 In April 2017, Defence initially assessed the financial risk as 'med-low', noting that the cost estimate for the full capability had not yet been developed. In November 2017, Defence reassessed the risk and increased it to 'high' as the cost to achieve the full capability was likely to exceed the available IIP provision. Defence noted that the risk would be mitigated by establishing a joint governance structure to enable efficient management of the budget across the total IIP provision for the Vetting Transformation and Case Management Projects, see Table 1.1.

2.50 In November 2017, Defence also advised the Investment Committee that cost estimates would be further developed through its market engagement activities and that capability versus cost trade-offs would be provided for Investment Committee consideration. The trade-offs identified and options that were developed are outlined in paragraphs 2.27 to 2.28.

### *Risk management plan*

2.51 The 2017 Defence Procurement Policy Manual, which was in effect during the project planning period, stated that for all procurements at or above the relevant procurement threshold Defence officials must:

undertake a risk assessment so that they are appropriately informed about the risks associated with the procurement; and subject to the risk assessment, develop and implement a risk management plan to manage the risks.

2.52 Defence developed a risk management plan for the project in 2021. There was no evidence that the plan was subsequently implemented or maintained. Implementation of approved risk management plans would assist Defence to actively manage the risks identified during the ‘Risk Mitigation and Requirements Setting phase’ of its complex and high value ICT projects.

### **Recommendation no. 1**

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.*

2.54 *Defence will perform reviews to ensure that risk management plans are approved and in place for all complex, high value ICT projects, with appropriate ongoing oversight and assurance structures.*

### **Did Defence establish effective governance, oversight and reporting arrangements?**

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.

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.

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.

2.55 According to Defence’s 2017 Capability Life Cycle Manual, project governance is executed through the Defence committees, governance documents and reporting requirements, and is comprised of decision-making fora, health checks and independent reviews, with decision-making delegated to the lowest appropriate level.

## Defence Committees

2.56 The Defence committees involved in approving and monitoring the Vetting Transformation Project comprised the Defence Investment Committee<sup>56</sup> and the Defence Communications and Information Systems Capability (DCISC) Committee.<sup>57</sup> The Defence Audit and Risk Committee (DARC) has also had a monitoring role.

2.57 The Investment Committee approved commencement of the project in April 2017, the recommended two-stage approval pathway, and the progression of the project through to first and second pass government approval. The Investment Committee considered the project on seven occasions between April 2017 and September 2020.

2.58 Whole of Defence oversight was to be provided by the DCISC Committee, which was established by the Defence Committee on 3 December 2018.<sup>58</sup> The inaugural meeting of the DCISC Committee was held on 20 May 2019 and its terms of reference were approved in July 2019. At January 2024, the DCISC committee had received seven updates on the project, with the last provided in June 2022.

2.59 Updates on the Vetting Transformation Project were presented to the DARC on three occasions between April 2022 and March 2023. The DARC was advised in April 2022 that the project was ‘tracking “RED” as a result of consequential impacts across architecture, security and gateway services’. In November 2022, the project status was ‘GREEN’ and the DARC was advised that the project was on track to deliver the initial operating capability on 28 November 2022. In March 2023, the DARC was advised that ‘the issues associated with the rollout of “myClearance” have been resolved, however a backlog [of clearances] remains’.

## Governance arrangements and decision-making forums

2.60 As discussed at paragraphs 2.2 to 2.6, governance arrangements for the Vetting Transformation Project were established in accordance with Defence’s Capability Life Cycle framework. Primarily designed to govern Defence’s acquisition and management of major military equipment, the framework outlines the governance arrangements and decision-making forums required at each phase of the Capability Life Cycle.

2.61 The arrangements established to oversee the Vetting Transformation Project were progressively amended over the life of the project in accordance with these requirements. Figure 2.6

---

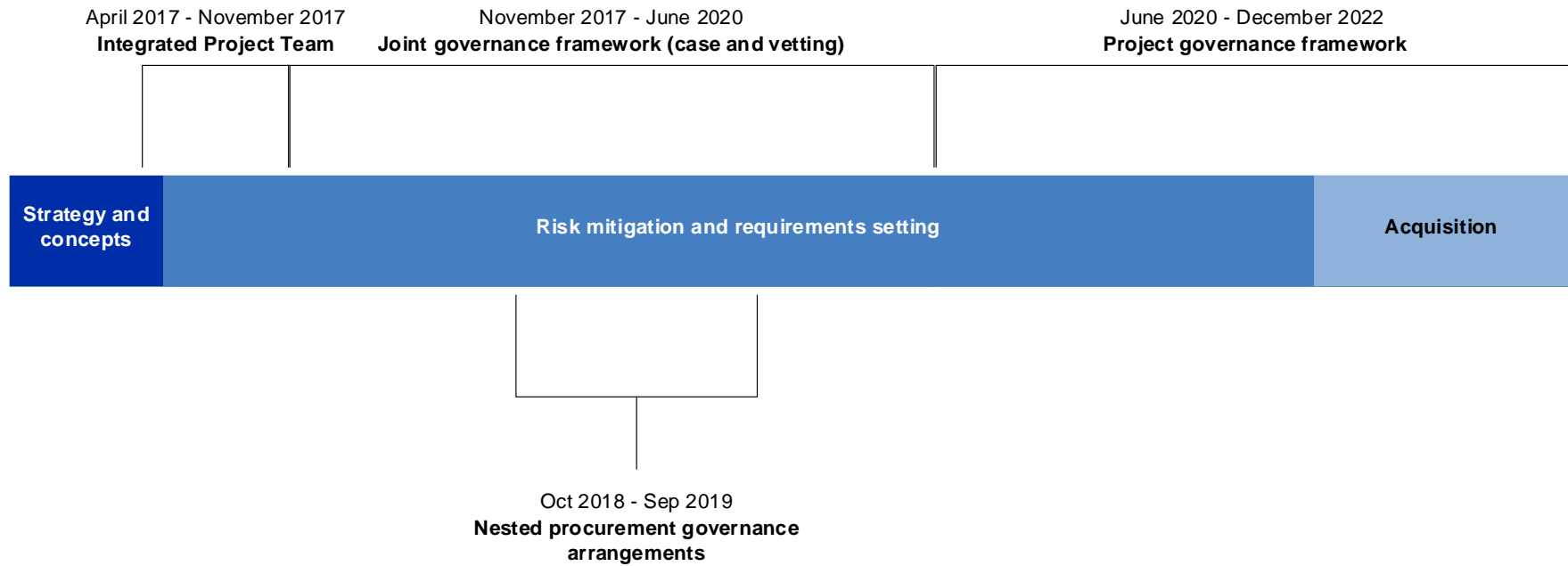
56 The Investment Committee is responsible for exercising strategic control over the investment portfolio and is the approving authority for the individual projects within the Integrated Investment Program (IIP). It is chaired by VCDF and its members include the Military Service Chiefs, Deputy Secretaries, Chief Finance Officer, Chief of Joint Capabilities and representatives of the Department of Finance, the Department of the Prime Minister and Cabinet, and the Office of National Intelligence.

57 The DCISC Committee is chaired by the Chief Information Officer and its membership includes Band 2/2 Star representatives from across Defence. It is the principal decision-making forum that approves the enterprise-level communications and information systems strategy to enable and develop Defence capability in line with strategic intent. It provides oversight of a program of work to prioritise, sequence and progress the delivery of integrated and secure information and communications management services, policy, performance reporting and assurance.

58 The Defence Committee is the most senior committee in Defence. It is responsible for setting top-level organisational goals and driving delivery of Defence’s commitments to the government and the community. The Defence Committee is chaired by the Secretary of Defence and its members include the Chief of the Defence Force, Vice Chief of the Defence Force, Associate Secretary, Chief Finance Officer, Deputy Secretary, Strategy, Policy and Industry and Chief of Defence Intelligence.

provides an overview of the changes to the project's governance arrangements between 2017 and 2023, across the first three phases of the Capability Life Cycle.

**Figure 2.6: Vetting Transformation Project — changes to governance arrangements between 2017 and 2023**



Source: ANAO analysis of Defence documentation.



### *Strategy and concepts phase*

2.62 The establishment of specific decision-making forums was not a Capability Life Cycle framework requirement during the strategy and concepts phase of the Vetting Transformation Project (December 2016 to April 2017). Nevertheless, in March 2017, the AGSVA Governance Board (AGSVA Board)<sup>59</sup> was asked to ‘endorse’ the key project documentation that had been developed for Investment Committee (Gate 0) consideration in mid-April 2017. While the AGSVA Board ‘noted’ the update, the minutes of the meeting did not state whether the planning documents had been endorsed as requested.

### *Risk mitigation and requirements setting phase*

2.63 After Gate 0 approval in April 2017, the project transitioned into the Risk Mitigation and Requirements Setting phase (April 2017 to September 2020). An Integrated Project Team (IPT) was established, as required by the Capability Life Cycle framework.<sup>60</sup> The IPT was overseen by and reported to the AGSVA Board. In September 2017 the board was asked to endorse updated versions of the three key project documents ahead of Gate 1 Investment Committee consideration in November 2017.<sup>61</sup> While the board noted the project update, the meeting minutes did not state if the documents had been endorsed.

2.64 In November 2017 Defence proposed, and the Investment Committee agreed, that joint governance arrangements would be established to oversee both the Case Management and Vetting Transformation Projects. As outlined at paragraph 2.19, Defence intended that the Case Management Project deliver technology for use by the Vetting Transformation Project. The arrangements for the Vetting Transformation Project included an expansion of the IPT into an Integrated Project Management Team (at the director or EL2 level), a Project Control Board (at the Band 1/1 Star level), and a Steering Committee (at the Band 2/2 Star level). Oversight continued to be provided by the AGSVA Board, which was supported by the Stakeholder Engagement Forum.<sup>62</sup>

#### Joint governance arrangements for the Vetting Transformation and Case Management Projects

2.65 In March 2018, high-level terms of reference (ToRs) to govern ‘all activities undertaken by the two [projects] from Gate 1 to Gate 2’ were developed. These arrangements were ‘to be revised in the lead up to transition from Gate 2 to implementation’.<sup>63</sup> The ToRs outlined the purpose and membership of each decision-making forum, comprising: individual Integrated Project Management Teams (IPMTs) and Project Control Boards; an Interdependency Management Working Group; and a Joint Steering Committee. The ToRs did not identify key roles, including the

59 The AGSVA Governance Board was established in October 2016 to provide strategic oversight of AGSVA and monitor the progress of service delivery reform and major systems development. The board includes representatives from across government and met on a quarterly basis between December 2016 and January 2024. Before the project received formal approval to commence in April 2017 (at Gate 0), the board had received two updates on the project.

60 Terms of Reference for the IPT were developed in May 2017 and endorsed in August 2017.

61 The planning documents that the AGSVA Governance Board was asked to endorse were the August 2017 versions of the Business Case, Joint Capability Needs Statement, and Project Execution Strategy.

62 The Stakeholder Engagement Forum is a whole-of-government working level consultation and discussion forum (at the Band 1/1 Star level) that provides members the opportunity to ‘inform the AGSVA Governance Board deliberations’ and ‘to ensure the consideration and protection of stakeholder interests in the AGSVA’s business strategy and implementation’.

63 Gate 2 approval was received from the Investment Committee on 16 September 2020.

CIO as the 'Technical Authority,' and the Architecture Management Review Board (AMRB).<sup>64</sup> The AMRB was responsible for endorsing the architecture and solution design (including the technological components) and the guidance to be issued to market.

2.66 The ANAO reviewed the documentation and ToRs for the individual decision-making forums under the joint governance arrangements and identified the following issues.

- The draft ToRs developed in 2017 for the IPT were not updated to reflect the joint governance arrangements until August 2020, when the ToRs for the IPMT were approved.
- ToRs for the Joint Steering Committee were not developed, and Defence did not retain adequate records of the activities and/or decisions of the Joint Steering Committee between April 2018 and April 2019.
- Interdependencies were to be managed in accordance with an interdependency plan. While this plan was drafted, it was not finalised, approved or implemented.

2.67 The joint governance arrangements were to be revised: in the lead up to Gate 2; and as the project transitioned from the risk mitigation and requirement setting phase to the acquisition phase (see paragraph 2.65). In October 2019, an Independent Assurance Review<sup>65</sup> (conducted one month prior to Gate 2<sup>66</sup>) found that while there were established governance forums, the decision-making ability and expectations of each were not clearly defined and a review of their effectiveness may be warranted (see paragraph 2.107).

2.68 In January 2020 the IPMT noted that the project's 'current governance arrangements did not appropriately ensure that key stakeholders were consulted as part of the pathway to [Investment Committee]' approval, and that the arrangements would 'be refreshed'. Work to refresh the joint governance arrangements commenced in January 2020, however in May 2020, Defence determined that the Case Management and Vetting Transformation Projects should be decoupled. The joint governance arrangements were subsequently dissolved and work commenced to revise the project governance arrangements.

Revised project governance arrangements

2.69 In June 2020, the Minister for Defence agreed that the Case Management Project would be delivered as part of Defence's Enterprise Resource Planning (ERP) Program and the Vetting Transformation Project would continue as a standalone project. To implement these arrangements, on 23 July 2020, the Project Steering Committee did the following.

- Endorsed the proposed split of responsibilities between the delivery lead (CIOG) and business sponsor (AGSVA) for the acquisition phase of the project, stating that:
  - architectural and solution design, legacy system decommissioning, ICT security, technical stakeholder engagement, and management of the systems integrator contract and other labour hire contracts would be the responsibility of CIOG;

---

64 The AMRB was established in 2016 as 'a cross Department function with representatives from all Capability Managers' and 'the single technology governance board for Defence ICT irrespective of the delivery agency'.

65 Independent Assurance Reviews, previously known as gate reviews, are internal reviews that can be initiated by the Capability Manager, Program Sponsor and/or Delivery Group. The reviews are conducted by an independently chaired review panel before all gates and critical milestones.

66 Gate 2 consideration by the Investment Committee occurred on 18 December 2019.

- the vetting operating model, policy, organisational change management and supporting procurement and contract management would be the responsibility of AGSVA; and
  - project management, governance, digitisation requirements, data cleansing, migration and archiving responsibilities would be shared, with CIOG accountable for the management of the integrated project management office and governance, and AGSVA accountable for data management.
- Endorsed a tiered governance model comprised of three AGSVA and CIOG co-chaired governance bodies: the Project Steering Committee (at the Band 2/2 Star level); a Project Steering Group (at the Band 1/1 Star level); and the Integrated Project Management Team (at the EL2 level).
  - Approved a decision rights matrix.

2.70 The Project Steering Committee (PSC) requested the development of the decision rights matrix ‘to provide clearer guidance on the approval authorities for Vetting Transformation Project decisions’. The matrix was focused on nine specific ‘decisions’ that remained unresolved at the time around affordability, technical and governance issues. This guidance was to be detailed in a Material Acquisition Agreement (MAA). As outlined at Table 2.1, an MAA was developed but not implemented or maintained.

2.71 The tiered governance model endorsed by the PSC in July 2020 (see paragraph 2.69) was not implemented.

- The Project Steering Committee (PSC) ToRs approved in August 2020 made no reference to co-chairing arrangements and the model in the ToRs did not align with the model endorsed by the PSC in July 2020.
- The October 2020 Integrated Project Management Plan (IPMP) made no reference to the Band 1 level Project Steering Group. It identified that the governance model for the project was comprised of the IPMT (Director or EL2 level) and PSC (Band 2/2 Star level), with oversight to be provided by the Enterprise Transformation Board.

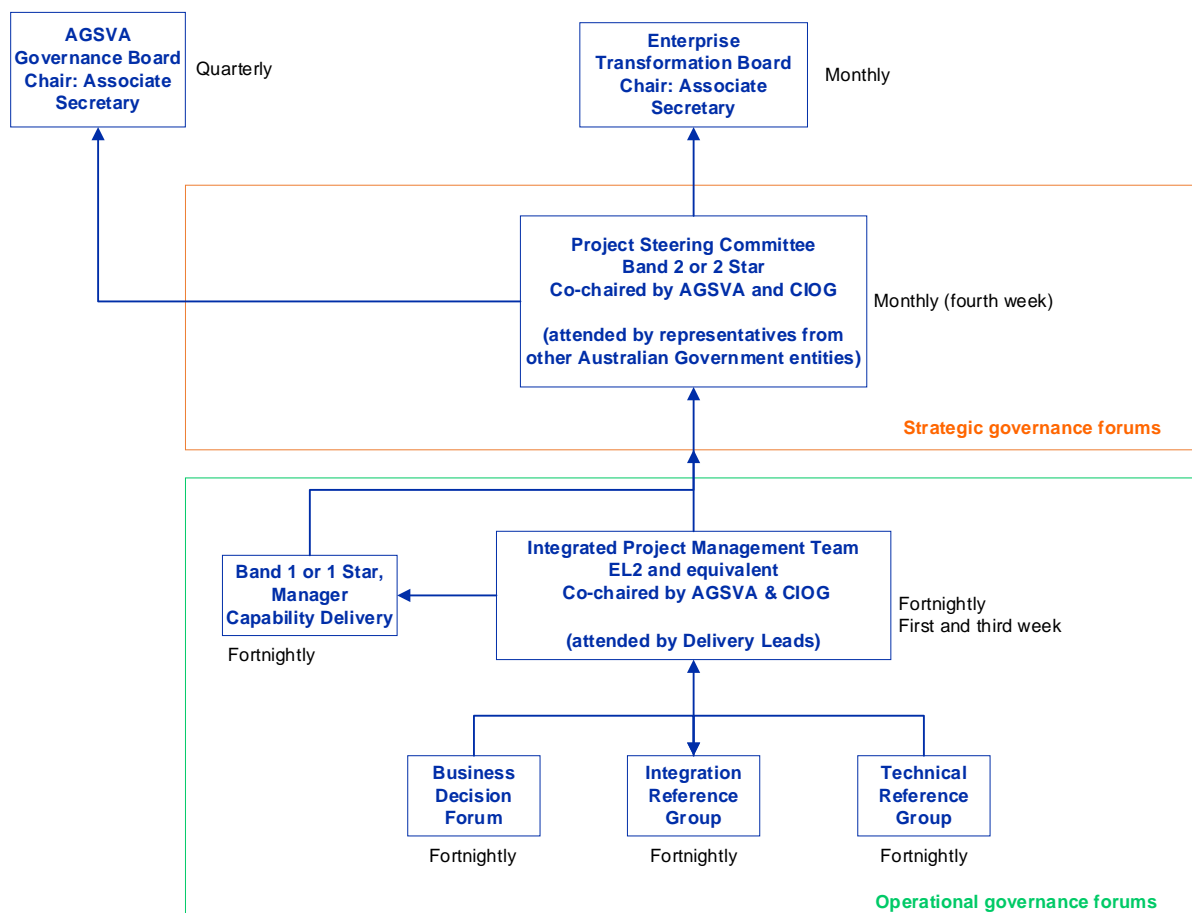
### *Acquisition phase*

2.72 The governance arrangements for the project’s acquisition phase were outlined in the Integrated Project Management Plan (IPMP) approved by the Defence Investment Committee in September 2020 (Gate 2). Defence records indicate that by the end of January 2021, the delivery framework and governance structure for the acquisition phase were under review. In March 2021, the PSC provisionally accepted a governance plan (developed by Deloitte).<sup>67</sup> The governance model in the plan is illustrated at Figure 2.7. This model was in place until December 2021.

---

<sup>67</sup> The PSC provided provisional acceptance of the governance plan pending feedback from the AGSVA business sponsor (First Assistant Secretary, Security & Vetting Services). There is no evidence that the feedback was provided or that the governance plan was formally accepted.

**Figure 2.7: Vetting Transformation Project governance arrangements — March 2021**



Source: ANAO analysis of Defence documentation.

#### March 2021 Governance Plan

2.73 The March 2021 governance plan outlined that decision-making was allocated to the following governance bodies.

- The Project Steering Committee (PSC) was ‘the key governance forum for direction and decision-making’ for the project. It was responsible for strategic control and providing senior management oversight ‘to ensure that the project is operating within specified parameters of scope, schedule and budget’.
- The Integrated Project Management Team (IPMT) was to manage ‘risks, issues and dependencies and [make] decisions that allow the project to progress in line with scope, schedule and budget’.
- The Business Decisions Forum (BDF)<sup>68</sup> was ‘a business led forum to escalate and validate key business decisions’ related to vetting business processes, operations and policy to support capability delivery.
- The Technical Reference Group (TRG) was to manage ‘technology and architecture design matters within the approved architectural boundaries and patterns’ and escalate matters

68 The Business Decisions Forum was to commence from 30 March 2021.

to the appropriate governance forum (including the Architecture Management Review Board, or AMRB).

- The Integration Reference Group (IRG) was to: review and manage ‘interdependencies between integration partners, including in-flight projects and external agencies’; and make ‘decisions that allow the project to progress in line with scope, schedule, and budget’.

2.74 The governance plan set out the purpose, membership and meeting frequency of the forums. It did not identify the reporting requirements, triggers or tolerances that would invoke the escalation process<sup>69</sup>, or the limit of decision-making powers of each forum. Further, between February and April 2021, there was no clear guidance on how ‘high’ risks were to be managed or which forum (the IPMT or PSC) was responsible for monitoring the effectiveness of actions to mitigate those risks. The integrated risk register indicates that ‘high’ risks were escalated to the PSC or the IPMT at the discretion of the project team. The risks were included in the Project Status Reports provided to the PSC (see paragraph 2.86).

2.75 The decisions made by the five decision-making forums were to be recorded in an integrated decision log. While a consolidated decision register was developed for the IPMT and PSC, separate registers were developed for the BDF and TRG. There is no evidence that a decision register for the IRG was developed. Further, the registers that were developed were not consistently maintained.

Amended governance arrangements

2.76 A Business Readiness Working Group (BRW)<sup>70</sup> and Project Steering Group (PSG) were established in October 2021.<sup>71</sup> These forums were not identified in the March 2021 governance plan discussed in paragraphs 2.72 and 2.73.

2.77 The BRW was established to provide ‘a forum for the Organisational Change Management team, Prime System Integrator (PSI) and the AGSVA Business Transformation teams to regularly meet, track and report on the progress of business change activities to achieve the Initial Operating Capability (IOC)’. The PSG was established to implement the following recommendation from an Independent Assurance Review (IAR) completed in September 2021.

Consideration be given to the establishment of a one Star Project Steering Group that includes representation from CIOG non-delivery divisions to support the timely and appropriate responses to Project needs.

2.78 In December 2021 the governance model (illustrated in Figure 2.7) was amended to include the PSG and BRW.

---

69 The escalation process was set out in the project management plan developed by the prime systems integrator (Accenture). The project management plan stated that ‘risks and issues requiring escalation and/or wider project visibility were to be documented in the integrated risk register and managed in accordance with the processes in the risk management plan. As outlined at paragraph 2.52, a risk management plan was developed but not approved or implemented.

70 The Business Readiness Working Group was to be chaired by the Director, Business Transformation, with representation at the EL2 level, however membership was limited to representatives from AGSVA and did not include any from CIOG. The working group initially convened in November 2021 and last met in December 2022.

71 The Project Steering Group was to be co-chaired by the Assistant Secretary, Vetting (AGSVA) and Assistant Secretary, Integration and Automation Delivery (CIOG) and first convened in December 2021.

2.79 In June 2022, the IPMT and PSG approved the conduct of a review of the project governance arrangements to: improve project operations, risks and issues management; address the ‘lack of clarity on the purpose of each forum’ (relating to information sharing and decision-making); and define and agree the level of authority delegated to each forum within the model. In August 2022, the project recommended disestablishing the IPMT and replacing it with Initial Operating Capability (IOC) and Final Operating Capability (FOC) forums and a Deployment Command Centre. While there is no evidence that the change was approved by the PSC, the model was implemented and in place when the system went live in November 2022.

#### 2023 Taskforce

2.80 In January 2023, after the myClearance system went live and the impact of the functionality issues became apparent (see paragraph 3.135), Defence established a dedicated taskforce to oversee the implementation of a remediation plan to rectify the issues encountered.

2.81 The project governance arrangements were paused until April 2023, when Defence resumed the ‘[f]ormal project governance ... alongside myClearance Taskforce oversight’. In July 2023, the project proposed re-establishing the governance arrangements comprising the IPMT, PSC and PSG.

#### August 2023 Post Implementation Review

2.82 In August 2023, Defence commissioned Axiom to undertake a ‘review of the implementation of myClearance’.<sup>72</sup> The governance and decision-making arrangements were examined as part of that review.<sup>73</sup> The review made the following findings.

- [The] project governance arrangements were not formally defined and maintained, including oversight, management and advisory committee structures. Further, the review team, noted there was a lack of clarity on the purpose of each forum within the governance model (e.g. information sharing and/or decision making) which potentially limited the effectiveness of project reporting and engagement with senior executives.<sup>74</sup>
- The review team observed multiple reporting lines and risk & issues registers across both CIOG and AGSVA without a single source of truth ... [further, the multiple registers] created an opportunity for inconsistencies.<sup>75</sup>
- [AGSVA] had limited technical ICT, Change Management, Data Migration, Business Reporting and Project Management capabilities and expertise, therefore requiring greater guidance and support by CIOG, the PMO [the Project Deliver Partner] and PSI [Prime System Integrator]. It was evident to the review team that the PMO took a very technical

---

72 Axiom is also contracted by Defence for the provision of internal audit services.

73 The post implementation review examined the following aspects of the governance arrangements: ‘decision making, appropriateness of accountability, transparency, performance reporting, risk management, agility and timeliness’.

74 As discussed in paragraphs 2.6 and 2.70, and examined in Table 2.1, key governance documents were not approved, implemented or maintained throughout the duration of the project. Further, the ToRs for each of the forums (noting that various governance models were established over the life of the project) did not clearly define or document interactions between the forums, including: their respective decision-making powers, escalation processes, relationships and reporting requirements (see paragraphs 2.66 and 2.71).

75 Defence’s use of multiple risk registers is discussed at paragraphs 3.63 to 3.66.

focus around the delivery of ICT solution (with the PSI) and solely left business readiness processes to AGSVA.<sup>76</sup>

2.83 The August 2023 review made seven recommendations to Defence to address the ‘Lack of clear Project Governance Oversight, duplicated Reporting and insufficient Resource Management’. Defence agreed to the recommendations and commenced a program of work to implement them.

2.84 In October 2023, the Project Steering Group (PSG) was advised that an end-to-end governance approach, aligned to the Defence Business Improvement Program (DBIP) had been completed and that the ToRs for each decision-making forum had been updated accordingly. These end-to-end governance arrangements included the establishment of a new DBIP Program Governance Board (to which the PSC, PSG and IPMT for the Vetting Transformation Project would report). The new arrangements were implemented in October 2023 but not all ToRs had been formally endorsed or approved. The ToRs for the new DBIP Program Governance Board were approved on 1 December 2023<sup>77</sup>, and as at April 2024, the revised ToRs for the PSG and IPMT have not been approved.

2.85 At March 2024, work to implement the recommendations of the Axiom review was ongoing, with all seven recommendations reported as ‘open’. In June 2024, Defence advised the ANAO that work remained ongoing to ensure that the recommendations have been implemented and can be closed.

### Reporting, review and assurance arrangements

2.86 The project reporting, review and assurance arrangements for the Vetting Transformation Project included the following.

- Provision of Project Status Reports to the Integrated Project Management Team (IPMT) and Project Steering Committee (PSC), with the reports provided to the Project Steering Group (PSG) from December 2021.
- Reporting to the Defence Communications and Information Systems Capability (DCISC) Committee, the Enterprise Transformation Board, the AGSVA Governance Board, and to government.

2.87 In line with Defence’s Capability Life Cycle framework, the project also underwent three Capability Manager Gateway Reviews and three Independent Assurance Reviews.

#### *Project Status Reports*

2.88 The Project Status Reports were provided at each IPMT and PSC during the period assessed by the ANAO (October 2017 to March 2024).<sup>78</sup> On average, the status reports prepared between February 2021 and November 2022 consistently rated six of the 14 components as ‘amber’ or ‘red’. This accurately reflected the issues being managed by the project, with examples as follows.

- In June 2021, the capability delivery issues were rated as ‘red’. This coincided with advice to the PSC that the solution architecture design for the IT system was being reviewed after

<sup>76</sup> Defence’s focus on the technical aspects of the IT system implementation is discussed in paragraphs 3.74 to 3.123.

<sup>77</sup> Defence advised the ANAO in April 2024 that the Terms of Reference for the DBIP Program Governance Board were approved by the Deputy Secretaries Board on 1 December 2023.

<sup>78</sup> Project status reports were also provided to the PSG once it was established in December 2021.

advice from CIOG that the project would adopt the whole-of-government Digital Identity Service (myGovID) in accordance with Digital Transformation Agency (DTA) guidance.<sup>79</sup> Further issues relating to the use of myGovID as the digital identity authentication method are discussed in paragraphs 2.92 to 2.96.

- In December 2021, the PSC noted that ‘the decision to pivot to myGovID [had] resulted in significant delays to detailed design activities’. The project status was assessed as ‘red’ due to the impact of delays in: procuring the required Government Furnished Materiel (GFM), including the infrastructure required to enable connectivity; and obtaining some of the security accreditations required to commence systems integration testing.
- In February 2022, the PSC was advised that the project had ‘forecast that it would exceed its agreed tolerances for schedule and budget due to unresolved dependencies and issues that were collectively delaying readiness to commence systems integration testing’.

#### Completeness of project status reporting

2.89 While project-level reporting accurately reflected the risks and issues being managed by the project team, the impact of the risks and issues on the expected functionality and capability of the system were not always clearly communicated to members of the PSG or PSC.

2.90 On 13 July 2022, the IPMT (EL2 level forum) was advised by the project team of ‘data quality issues requiring resolution’ and informed that if no action was taken, any clearance records affected ‘will not be viewable’. The IPMT was further advised that subsequent processes, such as clearance revalidations, ‘will also fail’ and that ‘this would inhibit AGSVA’s ability to manage these clearance holders’.

2.91 The PSG (Band 1/1 Star forum) was not informed, as the IPMT had been, of the impact that these data quality issues could have on the functionality of the system if not resolved. On 22 July 2022, the PSG was advised by the project team of ‘numerous known challenges with existing data states present in the current vetting database (PSAMS2) that may not migrate effectively into the new myClearance data model’. The PSG noted that the challenges around data migration, including those associated with date formats, were still being worked through. On 11 August 2022, the issue was included in the project status report provided to the PSC. The report also stated that the data migration status was ‘green’.

2.92 The impact of the architectural design decision — to require the use of a personal electronic device (such as a smartphone) for digital identity authentication (myGovID)<sup>80</sup> — was not brought to

---

79 The digital identity service included in Accenture’s tender response (and accepted by Defence) was the Australia Post Digital iD service. The June 2021 change to myGovID introduced technical risk and increased the schedule risk of the project as: a ‘test kit’ for early development was not available; a memorandum of understanding (MOU) between Defence and Services Australia needed to be in place for Defence to use myGovID; and testing of myGovID was not able to commence until the systems integration testing phase.

80 Personnel who work within Sensitive Compartmented Information Facilities (SCIFs) are unable to use myGovID as they are prohibited from having personal mobile devices in their workplace. Therefore, digital identity authentication methods that require a personal electronic device (mobile phone) to log in cannot be used. In February 2023, the myClearance taskforce advised that this issue impacted approximately 1,000 security officers and an alternate process to log in to the system was being examined.



the attention of the IPMT, PSG or PSC until November 2022, when the PSC discussed the need for alternate system access in secure environments.<sup>81</sup>

### *Ministerial and whole-of-government reporting*

2.93 In December 2020, Defence agreed that it would report annually on the status, risks and spend of the project to the Minister for Defence through Defence and whole-of-government mechanisms (including the Defence Enterprise Transformation Board and the AGSVA Governance Board).

2.94 This reporting was also incorporated into annual reporting prepared by AGSVA and provided to the Secretaries Board in 2020–21 and 2021–22. While the status of the project was reported, the risks and spend of the project were not included.

#### Digital two-factor authentication issue for users in secure areas

2.95 Defence provided an update on the status of the project a month before the 28 November 2022 launch of myClearance, in response to a request from the assistant minister in October 2022. The briefing included advice on accessing the myClearance system:

the use of myGovID will require workarounds for small number of users who do not have access to smartphones or other personal devices in their workplace for reasons such as security. The project team is working to develop a solution for these users but, given the significant security enhancement provided by myGovID, it was decided not to delay rollout until a solution was developed.

2.96 In response to the assistant minister's request for weekly reporting in the month prior to the launch, updates were provided on 9 and 17 November 2022. On 17 November 2022, Defence advised that:

AGSVA is aware that some myClearance Portal users may not typically have access to a smartphone (required for myGovID) in their workplace, for a variety of reasons, such as security. AGSVA is working through future access options for these impacted users, but these will not be in place at myClearance go-live.

2.97 To remedy the issues encountered after the system went live, including the system access issues for users in secure areas, a myClearance taskforce was established in February 2023. The minister was provided with weekly updates on the progress of the taskforce between March and July 2023.

2.98 The current status of the project and the extent to which the project is likely to deliver the capability uplift (as advised to government) is examined in Chapter 3.

---

81 In August 2022, Defence was advised by the Digital Transformation Agency that there were no immediate plans to support desktop use of myGovID or sending one-time PINs to email addresses to remedy the issue.

### *Capability manager gateway reviews*

2.99 Three Capability Manager Gateway Reviews (CMGRs) were conducted for the Vetting Transformation Project.<sup>82</sup> The first was held on 13 September 2017 and discussed risks to the proposed scope, schedule and budget of the project.<sup>83</sup>

2.100 The second took place on 12 June 2019, to discuss the coupled Case Management and Vetting Transformation Projects. Neither project was found to be ready for Investment Committee consideration. The project managers were directed to seek guidance — from the Associate Secretary (as the Capability Manager), the Architecture Management Review Board (AMRB), and the DCISC and Investment Committee as necessary — in order to:

- resolve critical project issues and agree an appropriate approval schedule;
- confirm the requirements for cross domain solutions, and quantify the costs and risks of implementing a different technological solution prior to integrating with SAP (being delivered by the ERP Program);
- confirm cost estimates, examine opportunities for delivery efficiencies, and assess overall affordability of the projects; and
- clarify responsibilities for data cleaning, quality, governance and migration.

2.101 The second CMGR process highlighted that due to the extent of the integration risks and dependency on other projects, the technology risk may be higher than ‘medium-high’. It also highlighted that integration issues were a key cost driver and noted that while a technology risk assessment had been done, it did not include an assessment of the integration risk.

2.102 The third CMGR was held on 12 August 2020, prior to Gate 2 approval in September 2020. It found that the project should proceed to the Defence Investment Committee for consideration, subject to five action items.<sup>84</sup>

### *Independent assurance reviews*

2.103 At April 2024, three independent assurance reviews (IARs) had been conducted over the life of the project: in October 2019, September 2021 and October 2022. Defence advised the ANAO in April 2024 that a fourth IAR, which was to be conducted in 2023, had been rescheduled to 2024.

2.104 The first IAR was conducted before the originally scheduled Gate 2 consideration in November 2019 and the second occurred after initial design (blueprinting) activities had concluded. The third IAR was conducted a month before the launch of the myClearance system.

---

82 CMGRs are independently chaired review panels, which are generally conducted before project approval gates and critical milestones to identify any outstanding issues that need to be addressed prior to Investment Committee consideration and to ensure that the project documentation and submission is fit-for-purpose.

83 As a result of the CMGR, the project was asked to update the project documentation to: include an evaluation of the options available to deliver the capability uplift; present viable options to address the funding shortfall; and identify how interdependencies with other projects would be managed.

84 These action items included updating the project documentation to: clearly define the capability being delivered; define the governance arrangements; explain the technical risk, transition, data remediation, and benefits management strategies; and update the cost model to include costs for Government Furnished Materials and accommodation requirements.

2.105 The three IAR reports consistently and accurately identified the risks and issues that eventuated and highlighted weaknesses in the governance and oversight arrangements of the project. For example, the first (2019) IAR found that:

The Project’s outlook for presenting a considered and measured proposal at IC [Investment Committee] and Second Pass consideration, and thereafter deliver the capability as planned to be high risk and unlikely.

There are established governance forums, however the decision-making ability or expectations of each are not readily evident ... A review as to the effectiveness of the current arrangements may be warranted.<sup>85</sup>

2.106 These concerns were expressed consistently in the two subsequent IARs, which also identified issues relating to: project affordability and schedule; the capability of the delivery lead (CIOG), resulting from over-reliance on contracted-in project management support to deliver the project; and the ‘aggressive testing cycle and approach to deployment’.

2.107 The second (2021) IAR found that by August 2021, the project was exposed to a ‘medium-high degree of technical risk’ and stated that the ‘schedule to IOC [Initial Operating Capability] remains under significant pressure, with a number of CIOG-dependent environment and security certification activities pressuring the critical path’. It was noted that the PSAMS2 system would ‘be required beyond FOC [Final Operating Capability], potentially for months or years, as a mitigation for extant data that may not cleanly migrate’. The following was also observed regarding Defence’s deployment strategy for the myClearance system.

The Deployment Strategy remains a work in progress, currently favouring a phased implementation (as opposed to a single big-bang) of AGSVA staff onto the new platform. A phased deployment strategy should mitigate a project risk of impacted or discontinued AGSVA service delivery, and alleviate resourcing pinch-points of User Acceptance Testing, Training, and accommodating the new system. Regardless of strategy, we foresee a likely impact to AGSVA workforce productivity, given the impact of committed AGSVA staff to training, User Acceptance Testing (UAT), system deployments, and familiarisation with new processes and systems.

2.108 In this context, the recommendations in the second IAR included the following.

The Project, on completion of the first attempt at production data<sup>86</sup> migration in September 2021, consciously assess and report if the data quality assumptions to date have proven correct, or if a change of strategy is required.

2.109 Due to various delays, including delays in providing the Government Furnished Materials (GFM) to the systems integrator (up to February 2022), the project schedule was re-baselined and the production data was not migrated into the new system until 28 October 2022.

---

85 The second (2021) IAR also highlighted governance weaknesses finding that:

the current Project Steering Committee is an appropriate and effective two-star governance forum. However, this representation may be restraining a more robust discussion and escalation of the apparent lack of CIOG corporate responsiveness to Project needs. The absence of a normal 1 star Project Steering Group, while understood, is not helpful and may warrant reconsideration.

86 The use of production data for testing purposes (that is, raw data from the PSAMS2 and ePack2 systems) provides the complexity needed for robust stress and performance testing. Due to the sensitive nature of the data held within the PSAMS2 and ePack2 systems, production data could not be used in development and test environments without de-identifying the data, or ‘masking’.

2.110 The third (2022) IAR was completed on 25 October 2022 and signed-off by the two responsible senior leaders (Band 2/2 Star) in AGSVA and CIOG by 8 November 2022. It found that the project had experienced ‘schedule challenges for the most part of this IOC phase’ and noted that ‘during the May [2021] IAR review, the critical path was at risk, and these risks have translated into realised delays’. The following four ‘characteristics’ of the project were noted:

- a. Execution of Systems Development, Systems Integration Testing (SIT), and User Acceptance Testing (UAT) concurrently, which are traditionally executed in series or with a slight overlap;
- b. Prolonged delays in the commencement and execution of Systems Testing and SIT, and a very condensed UAT schedule of 4 weeks (plus 2 weeks retest), noting as at the date of this report CIOG leadership advise that Systems Testing, SIT and UAT are well progressed and on track for completion;
- c. Several requirements scoped for IOC have been shifted to the second phase (FOC) with the prospect of further functions shifting in the weeks leading to deployment; and
- d. Physical connectivity risks, dependent on [Verizon], a third party, for carriage services. As at the date of this report, CIOG leadership advise that this risk is now resolved, with third party dependencies continuing to be actively managed by CIOG leadership.

2.111 The third (2022) IAR also stated that ‘these findings, and the condensed schedule will very likely result in issues of quality, late removal of user functionality or parts of the system that may fall short of end user expectations’. Despite these findings, the review noted that ‘Project stakeholders, inclusive of CIOG and AGSVA leadership, ... are aligned in their high level of confidence of IOC delivery on 28 [November 2022]’. In this context, the IAR stated the following.

We understand AGSVA leadership's risk appetite to accept a minimally scoped, bare-boned platform for IOC is very accommodating, knowing the step change improvements to be gained in productivity, efficiency, paper and transport reduction and data security, given the proposed digitisation of this process.

Consequently, the final decision to deploy IOC on 28 Nov 22 is a risk based decision, which must consider PMO [Project Management Office] provisioned quality metrics, UAT results, and an understanding of mitigations to all critical and high risks, for the AGSVA sponsor to make an informed decision, based on their risk appetite.

2.112 The actions undertaken by Defence to remedy the issues encountered after the system went live on 28 November 2022 are examined in Chapter 3, from paragraph 3.57.

## 3. Procurement and implementation

### Areas examined

This chapter examines the effectiveness of the Department of Defence's (Defence) procurement processes for the Vetting Transformation Project (myClearance) and its implementation.

### Conclusion

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.

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.

### Recommendations

The ANAO made one recommendation relating to system access and security and identified one opportunity for improvement relating to record-keeping during procurements.

3.1 Procurement by Commonwealth entities is subject to the Commonwealth Procurement Rules (CPRs), which are made under the *Public Governance, Performance and Accountability Act 2013*. Achieving value for money is the core rule of the CPRs, which state that procurements should (among other things): encourage competition and be non-discriminatory; and use public resources in an efficient, effective, economical and ethical manner.<sup>87</sup>

3.2 Defence required a range of contracted technical expertise and project management support to adequately resource the Vetting Transformation Project and deliver the myClearance

<sup>87</sup> Department of Finance, *Commonwealth Procurement Rules*, 13 June 2023, paragraph 4.4, [Internet] available at: <https://www.finance.gov.au/government/procurement/commonwealth-procurement-rules> [accessed 30 March 2024].

system. Defence’s relevant procurement activities were therefore central to the effective design and implementation of the myClearance system.

## Did Defence conduct effective procurement processes?

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.

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.

3.3 By the end of 2023, Defence had undertaken at least 30 procurements as part of the Vetting Transformation Project, to support its delivery of the myClearance system. This audit focused on four key procurements for the engagement of service providers critical to Defence’s resourcing for the project. These were the:

- contracted Project Approval and Support Services (PSS);
- Prime Systems Integrator (PSI);
- Organisational Change Management Partner (OCMP); and
- contracted Project Delivery Partner (PDP).

3.4 The procurement of the PSI was an area of focus in this audit as the PSI procurement process involved the most complexity and was critical to Defence’s delivery of the myClearance system.

### Procurement requirements and arrangements

3.5 Under the CPRs, an open tender process is required for procurements valued at or above the relevant threshold.<sup>88</sup> Some procurements are not subject to this particular requirement<sup>89</sup>, or

---

88 For non-corporate Commonwealth entities, other than for procurements of construction services, the threshold is \$80,000.

89 These exemptions are listed in Appendix A of the 2023 CPRs. These exemptions have been included in previous versions of the CPRs.

may not be subject to certain CPR requirements.<sup>90</sup> However, the overarching requirement to achieve value for money, which is the core rule of the CPRs, continues to apply.

3.6 Defence has developed internal policy and guidance documents to address the operation of the CPRs in the Defence context. Defence's March 2018 Complex Procurement Guide (which was in effect at the time of the selected procurement planning processes) stated that:

most military equipment and sustainment procurements are exempt from Division 2 of the CPRs, which provides Defence with the flexibility to conduct a 'limited tender' process for these kinds of procurements, but always subject to the overriding requirement to achieve value for money.

3.7 Defence's 2017 Procurement Policy Manual (in effect at the time of the procurement planning process for the Prime Systems Integrator) stated that when deciding on the procurement approach, officials 'must ensure that the method is commensurate with the scope, scale, and risk of the procurement and is consistent with value for money'.<sup>91</sup> Defence's procurement policy further stated that in circumstances where an open approach is not mandatory, 'Defence officials may still determine that an open tender process should be conducted as the best mechanism to deliver a value for money outcome'.<sup>92</sup> These requirements applied to each of the four procurements examined (see Table 3.1) and remained largely unchanged across the regular updates made to Defence's internal procurement policy framework between 2017 and 2022.

3.8 In respect to the procurements selected for ANAO review, Defence used three standing offer panels to engage four service providers. The CPRs provide that procurements from an existing standing offer are not subject to the rules in Division 2 of the CPRs, relating to an open tender process. However, these procurements must comply with the rules in Division 1 relating to achieving value for money.<sup>93</sup>

3.9 Defence also used existing Commonwealth commercial arrangements, whole-of-government procurement panels to source the hardware, software licences, and cloud hosting services for the project, and entered into 20 individual labour hire agreements. The labour hire agreements were used to: source the project director, contract manager, and subject matter

---

90 Paragraph 2.6 of the 2023 CPRs provides that the CPRs do not apply to the extent that an official applies measures determined by their Accountable Authority to be necessary for the maintenance or restoration of international peace and security, to protect human health, for the protection of essential security interests, or to protect national treasures of artistic, historic or archaeological value. This provision has been included in previous versions of the CPRs.

91 Department of Defence, *Defence Procurement Policy Manual*, December 2017, p.50. This provision remained the same in the November 2018 version of the manual (which applied to the OCMF procurements). The successor *Defence Procurement Manual* (first issued in July 2021) referred Defence personnel to the relevant Accountable Authority Instruction (AAI) on procurement. The AAI has consistently contained a similar provision:

value for money is achieved by:

- a. encouraging competition and non-discriminatory processes;
- b. using Commonwealth resources properly (efficient, effective, economical and ethical use of resources);
- c. making decisions in an accountable and transparent manner;
- d. considering and engaging with risks; and
- e. conduct a procurement process proportional to the scale and scope of the procurement.

92 *ibid.*, p.20.

93 See paragraph 9.12 of the 2023 CPRs. This provision has been included in previous versions of the CPRs.

experts; engage strategic, risk management, legal and probity advisors; commission a Program Assurance Review; and engage a project management team (see paragraphs 3.51 to 3.55).

3.10 Table 3.1 provides an overview of the selected Defence procurements and the panel arrangements used to engage the four service providers.



**Table 3.1: Vetting Transformation Project — selected procurements, panel arrangements and suppliers approached**

Services	Panel used	Suppliers approached	Description	Awarded to	Contract award date	No. of variations	Initial value <sup>a</sup> \$m	Current value <sup>b</sup> \$m
Project Approval and Support Services	Defence Professional Services Panel	7	Engaged to prepare the Business Case, Joint Capability Needs Statement and Project Execution Strategy and companion documentation required to achieve Defence Investment Committee approval to progress through each Gate (Gate 0, 1 and 2) and provide other project management support services.	Deloitte	18 Nov 2016	18	1.0	29.9
Prime Systems Integrator (PSI)	Defence's Information Communications and Technology Provider Arrangement (ICTPA)	15	<p>Contracted to provide the following services.</p> <ul style="list-style-type: none"> <li>• Systems Integration: the development and deployment of systems, including services relating to the connection and aggregation of disparate subsystems, functionalities or software applications to form one coordinated and functional system.</li> <li>• Application Services: the development, maintenance, support and service management of applications.</li> <li>• ICT Services: the engagement of specialist and niche providers as well as contractors to deliver discrete ICT services to satisfy specific business or technical needs.</li> </ul>	Accenture	31 Jan 2021	10	114.2	143.1

Services	Panel used	Suppliers approached	Description	Awarded to	Contract award date	No. of variations	Initial value <sup>a</sup> \$m	Current value <sup>b</sup> \$m
Organisational Change Management Partner	Defence's ICTPA panel	4	Contracted to assist Defence with organisational change management services associated with the deployment of the new vetting capability.	KPMG	1 Feb 2021	8	9.0	11.2
Project Delivery Partner	Digital Transformation Agency (DTA) Marketplace panel	1	The Project Delivery Partner was contracted to assist Defence in the project management and delivery functions.	VOAK Pty Ltd	6 Jul 2022	10	5.7	14.7
<b>Total</b>							<b>129.9</b>	<b>198.9</b>

Note a: The initial value is the contract value as recorded in Defence's approval documentation.

Note b: Publicly reported value on AusTender as at 21 March 2024.

Source: ANAO analysis of Defence documentation.

## Procurement of Project Approval and Support Services (PSS)

3.11 To procure the project support services, on 12 October 2016 Defence invited seven panellists from the Defence Professional Services Panel to respond to an RFQ for four ICT projects, including the Vetting Transformation Project. The selected panellists were given 10 business days to respond, with responses due on 26 October 2016. Of the seven panellists approached, five responded and two declined to respond.

3.12 The tender evaluation plan was approved on 21 October 2016.<sup>94</sup> On 3 November 2016 Defence selected the second highest ranked supplier (Deloitte) to provide project support services for the Case Management and Vetting Transformation Projects. The highest ranked supplier (KPMG) was engaged to provide 'Investment Committee Project Approval Services' for the other two ICT projects.

3.13 During the period reviewed by the ANAO (2016 to 2021), the contract was amended 18 times and the total contract value increased from \$1 million to \$29.9 million (GST inclusive). The approved Contract Change Proposals (CCPs) are listed in Appendix 6.

3.14 The CCPs were approved by an authorised delegate and were used largely to invoke options to extend in line with the overall objective and scope of the engagement. Four of the 18 CCPs introduced additional work packages and expanded the scope of the procurement to include the provision of:

- a SAP subject matter expert to assist with technical evaluation of responses;
- organisational change management services;
- additional market engagement activities;
- cost modelling; and
- operating model, architectural and cyber security subject matter experts.

## Procurement of the Prime Systems Integrator

3.15 The Prime Systems Integrator (PSI) had a primary role in the design and implementation of the new IT system. Of the four key procurements examined, the process to select the PSI was the most material in terms of complexity, cost and project delivery risk. At March 2024, the PSI engagement constituted \$143.1 million (72 per cent) of the \$198.9 million committed across the four procurements outlined in Table 3.1.

3.16 The Information Communications and Technology Provider Arrangement (ICTPA) panel was identified in May 2018 as the 'most viable panel' to procure the goods (hardware, software licences and cloud services) and services (the systems integrator and application development) required to deliver the IT system for the new vetting solution. The ICTPA panel came into effect on 13 July 2018.

3.17 The 2017 Defence Procurement Policy Manual (in effect at the time) stated the following.

---

94 The plan outlined that the evaluation of responses would include initial screening and shortlisting, individual assessment of tenders against the evaluation criteria and an assessment of value for money and final ranking of tenders.

- If a standing offer panel arrangement is established in Defence for goods or services, Defence officials must use the standing offer when procuring relevant goods or services, unless there is a valid reason for not doing so.<sup>95</sup>
- Defence officials must not use a standing offer panel arrangement to order goods or services that were not specified in the request documentation used to establish the arrangement, even if the relevant supplier may be able to provide the goods or services.

3.18 On 7 June 2018, the Chief Information Officer Group (CIOG) project team sought advice from Defence Legal on its proposed procurement approach, and assistance with drafting ‘Special Terms and Conditions to support the purchasing of software assets under the ICTPA’ panel. In mid-June 2018, Defence Legal advised that the procurement of an ‘end-to-end solution’ as contemplated by CIOG (that is, including the hardware and software) was not within the scope of the ICTPA and not covered by the terms of the deed.<sup>96</sup> This advice was reiterated in September 2018, when Defence Legal advised that ‘the best approach would be to go to open market for a complete end-to-end solution’. The concerns raised by Defence Legal related to:

- the appropriateness of the ICTPA panel as the procurement method; and
- the provision of hardware, software licences and cloud services not being within the scope of the ICTPA panel.

3.19 Defence approached the market for a systems integrator in October 2018 using the ICTPA panel. The procurement documentation required respondents to specify the various components required for their proposed solutions in a Bill of Materials (BoM). This was to be provided as an attachment to request for quotation (RFQ) responses. Defence intended to procure these items from existing Commonwealth commercial arrangements and/or whole-of-government procurement panels and provide them to the successful tenderer as Government Furnished Materials (GFM).

3.20 This approach differed from what Defence had advised panellists in September 2018, which was that suppliers did not need to include the pricing, or any terms and conditions associated with the goods required. The approach also resulted in suppliers needing to confirm with Defence whether the selected goods would be available from a panel arrangement, and placed an onus on Defence to provide accurate and timely information to all prospective suppliers.<sup>97</sup>

---

95 This requirement was updated in November 2018 to ensure that standing offers were to be used ‘unless a Group Head has approved not doing so’. This requirement remained largely consistent throughout the period examined in this audit. In May 2019, the requirement was included in Defence’s ‘Accountable Authority Instruction (AAI) 3 – Procurement’, which stated that: ‘Where a standing offer already exists within Defence that has been assessed as meeting the procurement requirement you must use the standing offer unless a Group Head has approved not doing so’. This requirement remains largely the same in Defence’s February 2024 AAls.

96 This position was consistent with Defence’s procurement policy, which stated that ‘Defence officials must not use a standing offer panel arrangement to order goods or services that were not specified in the request documentation used to establish the arrangement, even if the relevant supplier may be able to provide the goods or services’.

97 Paragraph 10.8 of the 2018 CPRs outlined that relevant entities must: ‘ensure that potential suppliers and tenderers are dealt with fairly and in a non-discriminatory manner when providing information leading to, or following, an approach to market’; and ‘promptly reply to any reasonable request from a potential supplier for relevant information about a procurement, and when responding to such enquiries must avoid a potential supplier, or group of potential suppliers, gaining an unfair advantage in a competitive procurement process’.

3.21 To enable the use of the ICTPA panel, extensive special terms and conditions were required to be drafted and inserted to allow for the purchase of software and cloud services, in addition to the systems integrator, application development, and ICT services.

3.22 The performance management framework for the ICTPA panel was designed for the sustainment of new and/or existing ICT systems. It is therefore not a fit-for-purpose performance management framework for the acquisition and sustainment of an end-to-end solution.

3.23 The performance measures in Defence's work order for the prime systems integrator include at-risk amounts, service level agreements, and Key Performance Indicators (KPIs). The performance measures do not apply to acquisition milestones or deliverables. There are no KPIs, 'stop' and/or 'incentive' payments that apply to the successful progression through entry and exit criteria.<sup>98</sup> The work order for the Vetting Transformation Project includes award term assessments and a liquidated damages mechanism.<sup>99</sup> This mechanism prioritised delivery of the system to the agreed schedule over the delivery of a system that would meet the requirements and deliver the expected capability uplift.

3.24 The RFQ for systems integration services was released to 15 panellists on 12 October 2018 and submissions were due on 7 December 2018. Of the 15 suppliers invited, three provided a response. Defence's requirements were structured and set out across five 'components' in the RFQ. Mandatory specifications were listed for each component.

#### *Evaluation process*

3.25 The evaluation process was outlined in the tender evaluation plan (TEP). The TEP was approved by the Chief Information Officer (CIO) on 5 December 2018 and stated that responses would be evaluated in a staged approach that included: initial screening; technical compliance; detailed evaluation; value for money assessment; and additional clarification activities (if required).

3.26 The purpose of the initial screening and shortlisting was to confirm that responses complied with the minimum content and format requirements. For responses to be considered further, a number of minimum content and format requirements were to be met, including the following.

- All goods (hardware, software and cloud services) proposed by the supplier must be procured from whole-of-government panels or extant Defence or Commonwealth agreements.
- SAP Investigative Case Management must be used as the proposed 'System of Record'.
- A costed Bill of Materials was to be included with RFQ responses.

3.27 Defence's 2017 Procurement Policy Manual, which was in effect at the time, stated that:

Defence procurements should not make significant use of minimum content and format requirements because of the consequences for a tenderer (and Defence) of not meeting such a requirement. Including unnecessarily specific minimum content and format requirements does not comply with best practice.

---

98 The entry and exit criteria provide assurance and are used to verify that the system has met the functional and non-functional requirements and will deliver the expected capability uplift.

99 If invoked, the liquidated damages were to be applied at a set amount per month for late delivery of IOC and/or FOC, capped at 10 per cent of the total charges for the services.

3.28 The screening and shortlisting report identified that two of the three responses submitted did not meet the minimum content and format requirements. One response did not contain the required Bill of Materials and one response contained rounding errors that breached the agreed labour rates ceiling and constituted a breach of the terms and conditions of the ICTPA deed. The report stated that these deficiencies were ‘unintentional errors of form’ and it was decided that all three responses would progress to more detailed assessment.

3.29 On 26 March 2019, the results of the individual, comparative, and value for money assessments were detailed in an interim systems integrator source evaluation report. The report included an assessment of the services and goods proposed by the suppliers to deliver the vetting solution.

- For the services, the report stated there was no clear best value for money response, and a number of gaps and issues requiring clarification were identified across all three responses.
- For the goods, no recommendation or ranking was provided due to the significant gaps, ambiguities and deficiencies that existed across all three responses.

3.30 In the report, Defence noted that it had been unable to determine which supplier had demonstrated a superior understanding of the requirement to identify the goods to be provided as Government Furnished Materials (GFM). On that basis, the report included a recommendation that all three suppliers progress to ‘Additional Clarification Activities’.

#### *Additional clarification activities*

3.31 Additional clarification activities were conducted between 8 and 17 April 2019. The workshops were used to ask clarifying questions and to enable prospective suppliers to demonstrate how their solutions would meet the functional and non-functional requirements (see paragraph 2.17). The additional clarification activities were also intended to: enable the evaluation teams to address risk; and clarify any uncertainties, inconsistencies or ambiguities contained in the responses.

3.32 The TEP stated that records of conversation would be retained.

3.33 While the agenda, presentation and outcomes of each workshop were documented, Defence did not prepare or retain the records of conversation as required. Documenting and retaining records of conversation with potential suppliers during a procurement enables Defence to demonstrate that its engagement activities are conducted in accordance with Defence policy and the CPRs, including requirements relating to probity and non-discrimination.

#### **Opportunity for improvement**

3.34 Defence would benefit from ensuring that records of conversation with potential suppliers during a procurement are documented and retained in accordance with Defence’s procurement policy framework.

#### *Parallel work order formation*

3.35 At the conclusion of the additional clarification activities, two suppliers progressed to parallel work order formation (or parallel negotiation) activities. Approval to progress to parallel

negotiations was provided by the CIO in June 2019. The objective of the negotiations was to formally agree to finalise and recommend for signature a work order between the Commonwealth and either for the supply of systems integration services.

3.36 Three parallel work order workshops were held with Accenture and another supplier between 2 and 17 July 2019 and a fourth workshop was held with Accenture on 22 July 2019. On 4 August 2019, Accenture was selected as the preferred supplier, and Defence agreed to suspend negotiations with the other supplier until work order formation negotiations were successfully completed. After the delegate approved Accenture as the preferred supplier, three more face-to-face work order formation sessions were held between Defence and Accenture between 7 and 22 August 2019 to: close the remaining commercial and technical issues; and agree planning assumptions to enable the provision of an updated price to address affordability issues.

#### *Joint delivery efficiency workshops*

3.37 In September 2019, Defence was advised that the Vetting Transformation and Case Management System Projects were unaffordable. Defence decided to address the affordability issues by exploring additional efficiency/cost reduction activities with the preferred supplier for the projects. Accenture, as the preferred supplier for both projects, was invited to participate in joint delivery efficiency workshops between 12 September and 16 October 2019. The workshops examined opportunities to: use common technology components, including infrastructure and ICT environments; consolidate resources through the merging of support teams; and bundle acquisition and sustainment work orders. At the conclusion of the workshops, Accenture submitted final revised pricing (on 31 October 2019) to reflect Defence directed and agreed changes to the scope and delivery approach.

3.38 In October 2019, a Defence Independent Assurance Review observed that ‘considerable work order formation definition (and hence pricing), is taking place after the announcement of a preferred supplier; i.e., after competitive leverage has been largely retired’.

#### *Analysis of alternatives*

3.39 As outlined at paragraph 1.9, the Defence Investment Committee did not agree to the project progressing to second pass in December 2019, due to affordability issues, and directed the projects to conduct further market research. In January 2020, Defence decided to ‘pause’ the procurements while it undertook analysis of alternative (AoA) activities.

3.40 On 9 January 2020 Defence met with Accenture to discuss the upcoming AoA. Defence records indicate that during the meeting, Accenture raised concerns that the AoA represented a new procurement process. The meeting record further indicated that Defence was offering Accenture ‘every opportunity to explore options for an affordable [case and vetting] capability and indeed to procure the capability through the existing processes’. On 10 January 2020, Defence wrote to Accenture and IBM, as the systems integrator for the Enterprise Resource Planning (ERP) Program, to advise them of Defence’s intention to conduct AoA activities to determine:

- the viability of delivering the Vetting and/or Case Management Projects through the ERP Program; and
- the extent to which the preferred tenderer (Accenture) could deliver a more affordable delivery option for the two projects through the existing procurement process.

3.41 On 13 January 2020, Defence sought probity advice regarding its decision to conduct AoA activities. The probity advisor<sup>100</sup> raised concerns with the potential changes in scope, noting that the implementation of a simplified technical solution did not comply with the mandatory requirements outlined in the RFQ released to market. The probity advisor also observed that deviating from the requirements in the RFQ, without providing the same opportunity to other shortlisted suppliers, could be seen as inequitable. In response, Defence told the probity advisor that the AoA, was considered to be a separate exercise, and was not part of the procurement activity, as the procurement process had been ‘paused’. The probity advisor acknowledged this information and observed that the activities must still be compliant with the CPRs.

3.42 As a result of the AoA activities, the following occurred.

- Defence provided the preferred supplier with the opportunity to develop a ‘solution to budget’ and submit costings for work it did not originally tender for.
- The process resulted in material changes to the technical solution, schedule and delivery approach tendered by the preferred supplier in December 2018.
- The process deviated from the directions provided to market in October 2018, which had mandated the use of SAP ICM as the system of record.

3.43 On 11 June 2020, the CIO (as delegate) authorised recommencing negotiations with the preferred systems integrator (Accenture) to deliver a proposal to meet a revised scope of work, including a simplified technical solution that did not comply with the mandatory requirements of the RFQ issued to market in October 2018. Accenture provided a revised proposal on 15 July 2020. The revised proposal included: changes to the technical solution<sup>101</sup> and business scope; whole of life pricing (10 years rather than 20 years); and a combined acquisition and sustainment contract.

3.44 Negotiations between Accenture and Defence continued until October 2020 regarding the performance framework; software licensing terms (procurement of the Pega Government Platform by Accenture and provided to Defence under a reseller model)<sup>102</sup>; milestone payments; indexation; warranty; and resourcing. After government provided second pass approval in December 2020 (see paragraph 1.12), Defence accepted the revised proposal and awarded the prime systems integrator contract to Accenture on 31 January 2021.

### **Procurement of Organisational Change Management Partner (OCMP)**

3.45 To procure the organisational change management services, Defence approached the market on 7 June 2019. Four panellists, selected from the ICTPA panel, were invited to respond to the RFQ. Responses were due on 28 June 2019. Of the four panellists approached, three provided a response.

3.46 Evaluation of the responses was conducted between July and August 2019 and the Tender Evaluation Report recommended that parallel work order formation activities be entered into with

---

100 The Probity Advisor originally contracted was from a company called Procurements & Contracts Division. At the time the advice was given to Defence, the company was trading under the name Pro Leaders Academy Consulting Professional Group Pty Ltd.

101 Using Pega as the System of Engagement and System of Record instead of Pega as the System of Engagement and SAP ICM as the System of Record as mandated in the RFQ issued to market on 12 October 2018.

102 The Source Evaluation Report stated that under this approach the Commonwealth was able to obtain substantially better pricing than otherwise available to Defence.



the first (KPMG) and second ranked responses. On 13 September 2019, KPMG and the second ranked respondent were invited to participate in parallel work order formation activities (contract negotiation).<sup>103</sup>

3.47 On 7 November 2019, KPMG was approved as the preferred supplier. The work order could not be awarded until the project received second pass approval from government. This approval was provided in December 2020 and Defence signed the work order with KPMG on 1 February 2021, see Table 3.1.

### **Procurement of Project Delivery Partner (PDP)**

3.48 Defence issued an RFQ for project delivery partner services, for both the Case Management and Vetting Transformation Projects, to three suppliers on the ICTPA panel in March 2019. Two suppliers responded. An evaluation report was completed by late July 2019, with the response from Deloitte ranked the highest.

3.49 Completion of the procurement was contingent on achieving Gate 2 approval from the Defence Investment Committee in November 2019 and second pass approval from government. This was not achieved, and the procurement was 'paused' in January 2020.

3.50 In May 2020, the Defence Investment Committee was advised that project delivery services would be provided by a public sector workforce augmented by contracted service providers, as required. In June 2020, Defence advised Deloitte that the project delivery partner services were no longer required, and the procurement was terminated.

3.51 When the 2016 contract with Deloitte (for project approval and support services) expired in June 2021, it was not renewed as the options to extend had been exhausted. Defence then engaged a project management support workforce of 14 members through individual labour hire arrangements until July 2022.

3.52 In July 2022, Defence engaged VOAK Pty Ltd to provide project delivery partner services as part of implementing recommendations from a Program Assurance Review commissioned in May 2022. Defence's processes for commissioning the assurance review and engaging the project delivery partner are examined in case study 1.

### **Defence's use of direct approaches to suppliers on panels**

3.53 Between 2016 and 2022, Defence awarded 20 contracts (valued at over \$22 million) to providers sourced from the ICTPA, Defence Support Services (DSS) and DTA marketplace panels. For 17 of those contracts (totalling \$20 million), only one supplier from the relevant panel was approached.

3.54 Defence's approach to panel procurement was not always consistent with:

- guidance material issued by the Department of Finance in July 2021 that stated 'wherever possible, you should approach more than one supplier on a panel for a quote. Even though value for money has been demonstrated for the supplier to be on a panel, you will still need to demonstrate value for money when engaging from a Panel'; and

---

103 There is no evidence that a Negotiation Directive was established to set the parameters and/or any limits with the procurement, as required by Defence's procurement policy framework.

- Defence’s procurement policy framework, including its Accountable Authority Instructions, which highlighted that the number of quotes sought should be sufficient to ensure Defence achieves value for money; and
- updated guidance in the CPRs (July 2022) and other guidance material issued by the Department of Finance, which stated that ‘to maximise competition, officials should approach multiple potential suppliers where possible’.<sup>104</sup>

3.55 Of the 17 contracts, two had reasons recorded for directly approaching a single panel supplier. One was awarded directly in accordance with the Indigenous Procurement Policy exemption.<sup>105</sup> The second was awarded directly on the basis that it was the only supplier with the skills to provide the services necessary to establish Azure Infrastructure at the PROTECTED level. For the remaining 15 contracts, the documented rationale was that ‘leveraging’ an existing panel ensured ‘that value for money is achieved’ and reduced the ‘administrative effort required’.<sup>106</sup> While this rationale addresses, in general terms, why Defence accessed panel arrangements, it does not address why only one supplier was approached for each of the 15 specific procurements.

3.56 Case study 1 reviews one of Defence’s 2022 processes to engage a single supplier from a panel to conduct a Program Assurance Review, fill a project director role, and replace the project management team (to provide project delivery partner services).

#### Case study 1. Defence’s commissioning of a program assurance review and subsequent procurements to engage a project director and project management team

In late March 2022, the First Assistant Secretary, ICT Delivery Division (an SES Band 2 officer in CIOG) met with a director from VOK Pty Ltd (VOK), a member of the DTA Marketplace panel (DTA panel). Defence did not prepare or retain a record of this meeting. On 11 April 2022, Defence directly approached VOK through the DTA panel to conduct a Program Assurance Review of the Vetting Transformation Project.

Defence’s July 2021 *Accountable Authority Instruction (AAI) 2 Spending Defence Money – Procurement*, which applied at the time, stated that: ‘For panels/standing offer arrangements established by Defence you must use that arrangement unless a Group Head or Service Chief has approved otherwise or you are procuring from an indigenous supplier’ (see the earlier discussion in paragraph 3.17). At the time of the procurement, VOK was not a member of the

<sup>104</sup> Department of Finance, *Procuring from a Panel – Panels 101*, paragraph 9, [Internet], Finance, available from <https://www.finance.gov.au/government/procurement/buying-australian-government/procuring-panels-panels-101> [accessed 22 March 2024]. Paragraph 9 of his guidance states that:

As advised at paragraph 9.14 of the CPRs, wherever possible, you should approach more than one supplier on a Panel for a quote. Even though value for money has been demonstrated for the supplier to be on a panel, you will still need to demonstrate value for money when engaging from a Panel, and competition is one of the easier ways to demonstrate this.

- a. Where you only approach one supplier, you should provide your delegate with reasons on how value for money will be achieved in the procurement.

<sup>105</sup> The contract was for a technical assurance lead. The documented rationale in the PGPA section 23 approval stated that the engagement was valued at less than \$200,000 and the Indigenous Procurement Policy applied as the services were to be sourced from an indigenous supplier. This supplier was contracted five times for the projects and directly contracted for four of those five times.

<sup>106</sup> The ANAO reported on a similar approach of using panels to engage single suppliers from panels and ‘leveraging’ existing contractual arrangements in Auditor-General Report No. 5 of 2022–23 *Digital Transformation Agency’s Procurement of ICT-Related Services*, paragraphs 3.22 to 3.43 and 4.39 to 4.41.

ICTPA panel and the use of the DTA panel to engage VOAK for the assurance review was approved by an SES Band 1 officer in CIOG. This was a breach of Defence's AAI as these services were available from Defence's ICTPA panel, VOAK is not an indigenous supplier and approval from a Group Head or Service Chief to use the DTA panel for the procurement had not been obtained.

The approval documentation did not record why the services could not be procured from the ICTPA panel. The documented rationale stated that 'VOAK Group has been identified as having skilled personnel available to deliver the requirements of the project within the timeframes available, with proven experience and expertise in Digital Identity and myGov technology platforms which is relevant to the ICT deliverables'. Defence issued the RFQ to VOAK on 21 April 2022, with the response due on 26 April 2022. The five-day response period included a weekend and a public holiday.

The Program Assurance Review report was submitted by VOAK to Defence on 8 June 2022. It stated that overall, confidence in the ability of the project management team (made up of individually contracted-in service providers) to deliver the project on time and on budget was low and made eight recommendations. The first recommendation was that Defence source a new project management team.

On 1 June 2022, VOAK contacted the SES Band 1 and 2 officers in CIOG and offered to fill, on a temporary basis, the Project Director role that was due to be vacated by the incumbent provider. This offer constituted an unsolicited proposal. Defence's procurement policy framework contains the following guidance on the handling of unsolicited proposals:

Prior to undertaking a desktop review of an unsolicited proposal, Defence officials should seek specialist contracting or legal advice and establish appropriate probity protocols and arrangements to govern the review of the unsolicited proposal ...

Defence did not seek specialist advice and did not establish any probity protocols for the handling of the proposal. Defence accepted the offer on 1 June 2022 'pending a procurement process to backfill this position'. The subsequent procurement process involved Defence directly approaching VOAK to provide the services on 9 June 2022. The contract was awarded for an initial period of six months for \$258,720 (GST Inclusive) on 30 June 2022 and included options to extend for two more periods of up to six months each (12 months in total). At December 2023, both options had been invoked and the total value of the contract had increased to \$846,720 (GST Inclusive).

When developing the scope of work to establish a new project management office in early June 2022, Defence sought the assistance of VOAK. Defence then issued the RFQ for a replacement project management team to VOAK on 24 June 2022, which was before approval to approach the market was provided on 28 June 2022. Defence awarded the contract to VOAK on 6 July 2022 to engage a project management team of 13 personnel to provide project delivery partner services for 12 months (220 days) at an initial cost of \$5.7 million (GST Inclusive).

At May 2024, across the three contracts with VOAK, 14 changes had been approved and the total committed funds had increased from \$6.2 million (GST Inclusive) to \$15.9 million (GST inclusive). Defence also extended its Project Director and Project Management Office (Project Delivery Partner) contracts with VOAK to support the provision of services beyond the Vetting

Transformation Project to another Defence ICT transformation project, the Health Knowledge Management System.

## Did Defence effectively manage implementation?

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.

- 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.
- 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.
- 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.

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.

## Project management planning

### *Integrated Project Management Plan (IPMP)*

3.57 Defence's Capability Life Cycle framework requires that an Integrated Project Management Plan (IPMP) be developed by the project team and endorsed by the Project Sponsor (Assistant Secretary, Vetting). The IPMP describes the activities required to successfully manage delivery of a project and is to be finalised before the project progresses to the acquisition phase of the Capability Life Cycle. The IPMP is then to be updated on an annual basis.<sup>107</sup>

3.58 The IPMP for the Vetting Transformation Project was initially developed in August 2017, further refined between May 2019 and September 2020, and was last updated on 28 October 2020, see Table 2.1. At February 2024, the IPMP was not finalised or signed by the Project Sponsor.

3.59 The IPMP was not maintained as required. A project management plan (PMP) and integrated project schedule (IPS) were developed in mid-2021 by the contracted prime systems integrator (Accenture) to monitor and manage the delivery of the new vetting system

---

<sup>107</sup> Figure 2.1, illustrates the timing and duration of the four phases for the Capability Life Cycle for the Vetting Transformation Project.

(myClearance). The PMP was a deliverable under the contract with Accenture and its stated purpose was to align with, not replace, the IPMP.

### *Project Management Plan (PMP)*

3.60 The PMP was approved in May 2021 and detailed the process to design, build, test and deploy the new vetting system. It identified that the Vetting Transformation Project would be delivered in two modules across four phases: mobilisation; blueprinting; transformation; and sustainment.

- Module one — the core vetting system, which constituted Initial Operating Capability (IOC).
- Module two — the continuous assessment module, constituting Final Operating Capability (FOC).

3.61 Figure 3.1 maps the four phases of the project against the systems development lifecycle.

- The mobilisation phase commenced in February 2021 and was completed in March 2021.<sup>108</sup>
- The blueprinting phase (for module one) commenced in February 2021 and was completed by the end of June 2021.<sup>109</sup>
- The transformation phase (build, test and deployment for module one) commenced in July 2021 and was completed in July 2023.<sup>110</sup>
- The sustainment phase was originally due to commence in August 2022, 18 months after contract commencement.<sup>111</sup> It commenced in December 2022 after the core vetting system (module one) went live, was ongoing at March 2024, and is planned to continue for the life of the capability.

---

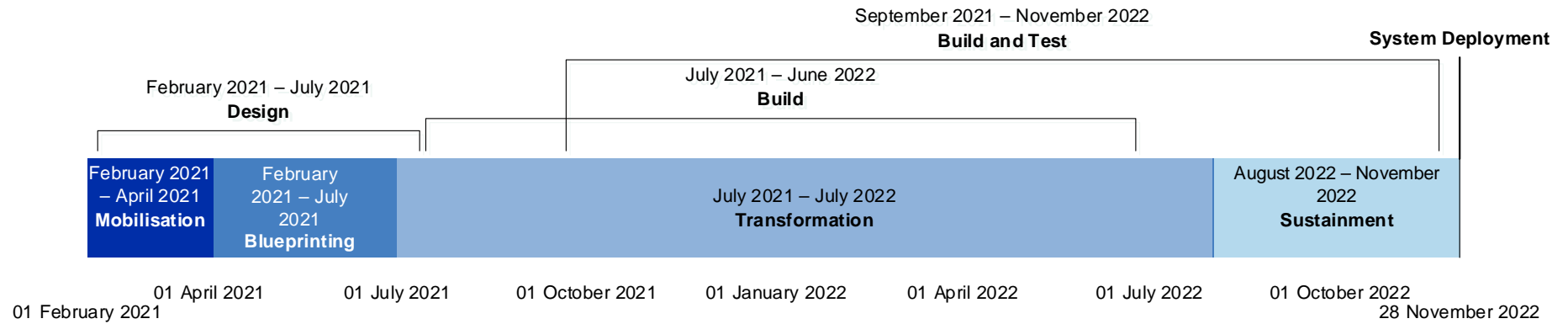
108 Mobilisation of the project included establishing the people, processes, plans, infrastructure, and software required to commence design, build and testing activities.

109 Blueprinting activities sought to elicit the necessary insight that informed how the solution would be fit for the end users, and not just the vetting process.

110 Transformation activities focus on the development of the computer system using a hybrid waterfall methodology. The transformation phase also includes decommissioning the old system, data migration, organisational change and benefits tracking.

111 Sustainment activities will focus on the ongoing support, maintenance and operation of the system.

**Figure 3.1: Planned approach to deliver the core vetting solution**



Source: ANAO analysis of Defence documentation.

3.62 In December 2023, the Associate Secretary agreed that Major Release Two, released on 28 July 2023 delivered the uplift in myClearance capability required to align with the Initial Operating Capability requirements, as advised to government, and that the Final Operating Capability (build, test and deployment for module two) had been technically met.

### *Risk management*

3.63 The PMP identified that the process used to manage risks, issues and dependencies would be detailed in a risk management plan and logged in an integrated risk register.

3.64 While the risk management plan was developed, it was not approved or implemented.

3.65 A risk and issues register and dependency tracker were developed and reviewed on a weekly basis between March 2021 and November 2022. The risk register identified the categories of risk, whether the risk was associated with IOC or FOC, the risk owner, the status, escalation pathway, impact and treatment of the risk. The register did not identify the triggers and tolerances to invoke the escalation pathway. The risk register was included in weekly project reporting and the Project Status Reports (see paragraph 2.88).<sup>112</sup>

3.66 As discussed in paragraphs 2.88 to 2.92, the risks, issues and dependencies were accurately reflected in project reporting and were consistently rated as ‘red’ or ‘amber’ between March 2021 and August 2022. These issues were not resolved in a timely manner, and while the information provided to the Integrated Project Management Team (IPMT) and Project Steering Committee (PSC) detailed the cause of the delay in technical terms, the likely impact on the functionality or capability of the system was not made clear. Reporting on such impacts supports informed and risk-based decision-making.

### *Integrated Project Schedule (IPS)*

3.67 In addition to the PMP, the systems integrator developed an IPS that was delivered in March 2021. The IPS has been re-baselined on four occasions.

- September 2021: to reflect changes to the schedule from blueprinting activities completed in July 2021, and the planned IOC date from July to September 2022 (see paragraph 3.78).
- May 2022: to reflect changes to the schedule agreed by the PSC and to implement the recommendations of the project exception report (see paragraph 3.89).
- November 2022: to reflect the activities required to achieve FOC.
- May 2023: to reflect a change in the delivery approach from an IOC/FOC model to a major and minor release model.<sup>113</sup>

3.68 According to the PMP, the IPS was to be considered the ‘single source of truth’ and updated weekly. The IPS was maintained and included in the weekly reporting developed by the systems integrator. Not all updates were consistently applied to the IPS. This meant that accurate longitudinal analysis to identify trends and/or impacts to the schedule over time was not possible.

---

112 At May 2024, the systems integrator continued to provide weekly reporting to the project. The focus of weekly reporting has been updated to reflect the sustainment phase of the project.

113 The fourth re-baseline implemented changes to the Capability Life Cycle and delivery approach for major ICT projects, as recommended by the 2023 Defence Strategic Review (DSR). A public version of the DSR was released by the Australian Government on 24 April 2023.

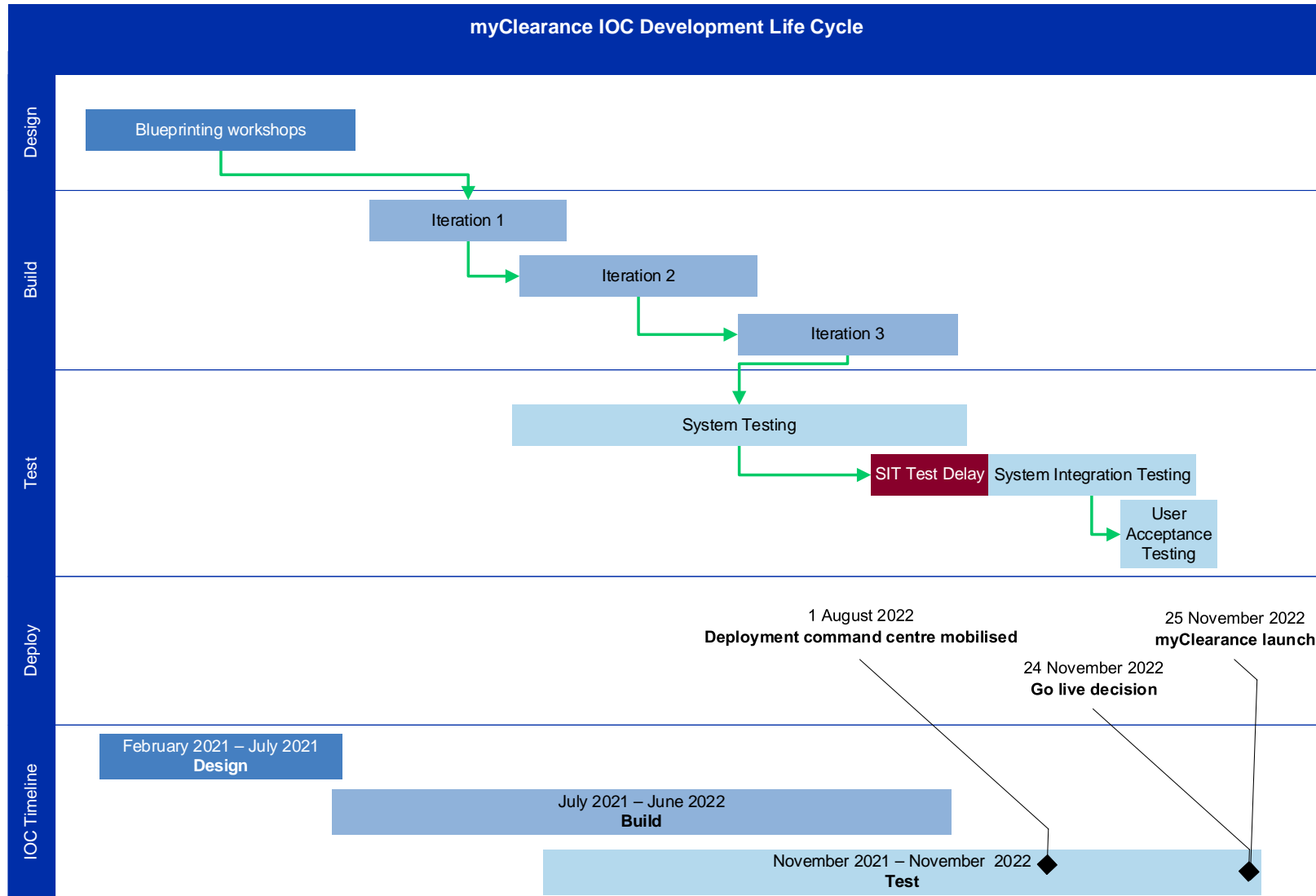
The IPS was aligned to the deliverables of the systems integrator contract rather than mapped to the tasks in the project or the systems development lifecycle phases.

### **Systems development**

3.69 The process used to design, build and test the system, prior to its launch on 28 November 2022, is outlined at Figure 3.2.



**Figure 3.2: myClearance development life cycle — Initial Operating Capability (IOC)**



Source: ANAO analysis of Defence documentation.

### *Mobilisation activities*

3.70 Mobilisation activities were conducted between 1 February 2021 and 31 March 2021 (see paragraph 3.61). These activities included on-boarding the workforce, and identification and provision of the goods (hardware, software, cloud services) required to design, build, test and deploy the vetting system.

3.71 The Project Steering Committee was advised in March 2021 that completion of the mobilisation activities was ‘at risk’ due to delays encountered in procuring the hardware, software and cloud services required for the myClearance system. This advice was consistent with a ‘mobilisation report’ provided by the PSI on 15 April 2021. The PSI was responsible for producing the mobilisation report in accordance with the executed contract/work order. The report was approved by Defence on 6 May 2021.<sup>114</sup>

3.72 In February 2022, twelve months after the mobilisation phase commenced, the risks and issues identified in the 15 April 2021 mobilisation report had not been resolved. The project advised the PSC that it was ‘forecast to exceed its tolerances for schedule and budget due to unresolved issues that were collectively delaying readiness to commence systems integration testing’ (see paragraph 2.88).

### *Design activities*

3.73 To design the system, the project was to complete blueprinting (preliminary design) and detailed design activities. The design phase also included defining the digitisation, data migration and security accreditation requirements; securing the hardware, software, and cloud services; and commencing foundational build activities.

3.74 Blueprinting for the core vetting module (module one) commenced on 12 March 2021 and concluded on 30 June 2021 (see paragraph 3.61). The purpose of the blueprinting activity was to validate the functional and non-functional requirements developed during the planning phase of the project. Blueprinting for the continuous assessment module (module two) was scheduled to commence in April 2022. The project was to conduct blueprinting workshops between June and August 2022 to define the scope for FOC, including continuous assessment, integrations, enhancements, and deferred requirements from IOC.<sup>115</sup>

3.75 The work to design both modules of the future state vetting solution was undertaken by individuals and working groups, including a core design team. The core design team was comprised of representatives from Defence, Accenture and KPMG and reported to the Business Decisions Forum (BDF) and the Technical Reference Group (TRG) in accordance with the project governance model illustrated in Figure 2.7.

3.76 During the blueprinting activities, changes to the functional requirements were documented in an updated requirements traceability matrix. Design decisions were to be logged in the requirements traceability matrix and a decision register. Between April and June 2021, seven ‘decision makers’ were recorded in the matrix: AGSVA; the BDF; the TRG; the core design team; the

---

114 The mobilisation report documented the readiness of the project across five elements (people, infrastructure, governance, vetting, and software/applications) required to commence design, build and testing activities for the replacement ICT system.

115 By November 2023, Defence recommended that the government agree to de-scope some of these features, including the continuous assessment component (discussed at paragraph 3.139).

Solution Architect (Prime Systems Integrator); the Assistant Director, Business Transformation; and a group of three individuals.<sup>116</sup> Of the 158 decisions logged in the matrix:

- 18 (11 per cent) were made by the BDF;
- 17 (11 per cent) were made by the core design team;
- 40 (25 per cent) were made by the Director, Business Transformation and the solution architects;
- 16 (10 per cent) were marked as duplicates and ‘covered by other decisions logged’;
- seven (four per cent) were made by AGSVA, the Technical Reference Group, or the solutions architects; and
- 60 (38 per cent) had no decision maker recorded.

3.77 As a result of the 60 entries where no decision maker was recorded, the matrix and decision log (see paragraph 2.75) were incomplete and an accessible and transparent record of decision-making was not retained.

3.78 The Integrated Project Management Team (IPMT) was to ‘review’ and ‘agree’ with the decisions made by the BDF and TRG. In May 2021, the IPMT agreed to changes to the design of the system as recommended by the BDF.<sup>117</sup> On 30 July 2021, the PSC approved revisions to the: vetting solution; the capability to be delivered at IOC; and the agreed schedule. The decision brief recommended: a four per cent increase to requirements and a six per cent increase in the number of interfaces; a three month extension to the scheduled go-live date from July 2022 to September 2022; and replacing the digital identity service to be provided by Australia Post with the myGovID digital identity service (see paragraph 2.88).

### *Build phase*

3.79 The build phase commenced in July 2021 and was originally scheduled to take 24 months (July 2021 to July 2023). The build process involved converting the functional requirements (which were outlined in the approach to market in 2018 and confirmed through the blueprinting activity) into user stories that were then used to define what was to be built and tested in each iteration.

3.80 The core vetting solution was to be built in three iterations.

3.81 The objective of the first iteration was to build the end-to-end functionality to support the baseline security clearance process for 12 categories of users.<sup>118</sup> The build of the first iteration commenced in July 2021 and was completed in October 2021.

---

116 The three individuals were the Director, Business Transformation and two Solution Architects, one engaged by Defence and one by the Prime Systems Integrator. All were members of the core design team.

117 IPMT members ‘agreed to remove Google Maps visualisation from the scope’ and ‘agreed to replace the IAM authentication interface with Active Directory to authenticate users within Defence and provide access to the Vetting system’. IPMT members also ‘agreed there [was] no requirement for a Decision Brief to PSC [Project Steering Committee]’ on the changes.

118 The users included: clearance subjects; security officers; authorised decision makers; vetting officers; and administrators.

- The build completion report, submitted in November 2021, identified 18 build defects to be resolved, including system functionality, accessibility, and information exchange issues between the ‘portal’ and the ‘platform’.<sup>119</sup>

3.82 The build of the second iteration commenced in October 2021 and concluded in February 2022. Three build completion reports were submitted.

- The first report was for the portal and platform integration, which identified 22 build defects. Of the 22 defects, eight (37 per cent) were carried over from iteration one, and 14 (63 per cent) were new. The defects identified were largely associated with the exchange of information between the portal and the platform, the interfaces with other Defence applications and systems, and the internal and external integrations (including integration with the Attorney-General’s Department (AGD)).
- The other two reports were for the reporting module (PowerBI) and the records management module (OpenText).
  - The report for the reporting module identified four build defects. Two (50 per cent) were related to the availability of information in the platform and the quality of the test data. One was related to the need for additional data points for specific ‘user stories’ and the other was related to reporting through Microsoft PowerBI.
  - The report for the records management module identified three defects. These related to the quality and format of the data to be transferred from the previous system (PSAMS2 and ePack) into the records management module (OpenText) of the new system.

3.83 The build of the third iteration commenced in March 2022 and concluded in June 2022. The PSC was advised in June 2022 that the build completion milestone had been met, marking the completion of the design and build phases of the myClearance system to deliver IOC.

3.84 The IPMT and PSC were kept up to date on the progress of the build and in approving changes to the design. As outlined in paragraphs 2.89 to 2.92, the IPMT and PSC were not advised of how risks impacting the build process would be managed or what the impact on the functionality of the system would be. For example, in December 2021 the PSC (the SES Band 2/2 Star committee responsible for the project) was advised that:

the Vetting Transformation solution is architected to integrate with AGD to enable information sharing for clearance assessments. This was originally planned as a direct replacement of the existing integration. During blueprinting, AGSVA and AGD advised the project that an enhanced information flow would be required in the future. As delivery timeframes and requirements were uncertain, the project retained the existing for IOC and scoped an enhanced set of integrations for FOC. The current BAU integration will not align with the enhancements that have been designed and built in the VT [myClearance] system.

3.85 In other words, the planned data sharing between the AGSVA and AGD systems could not be delivered as part of the core vetting system, and delivery of that capability was delayed to a later stage of the project. This aspect of the project was later de-scoped in November 2023 (see paragraph 3.139).

---

119 The report outlined a distinction between the ‘VT [Vetting Transformation] Portal which sits in the Unofficial domain for external users and the VT Platform which sits in the Protected domain for internal users’.

3.86 The PSC ‘noted’ the two options proposed and ‘endorsed’ the recommended option that the existing integration would be retained for IOC and the misalignment addressed for FOC. The PSC was not informed of what this meant in terms of its impact on the functionality and capability of the system and the personnel security vetting process. It meant that the AGD/Australian Security Intelligence Organisation (ASIO) systems would not be able to process the information sent from the myClearance system (transfer cases) to conduct security assessments when the system went live in November 2022.

### *Sourcing infrastructure*

3.87 As outlined in paragraph 3.19, the infrastructure (hardware and cloud services) required for the build was to be sourced by Defence and provided to the systems integrator as Government Furnished Materials (GFM). The infrastructure was to be procured during the mobilisation phase from 1 February 2021 to 31 March 2021 (see paragraph 3.70).

3.88 Between February and May 2021, the PSC was provided regular updates which addressed the delays in providing GFM and the impact of those delays on the project’s critical path. The PSC was advised as follows.

- In February 2021 — that the infrastructure team was unable to start the build.
- In March 2021 — that an architectural decision had been made to provide the project with ‘interim non-production’ Official and Protected environments, and a sandpit environment, to reduce ‘the raw delay of 7 weeks to 2.5 weeks’, as the enterprise cloud design was still maturing and a production environment was not yet ready.
- In May 2021 — of the delays in providing the hardware and cloud services to the systems integrator as GFM.

3.89 The delays in providing GFM continued to February 2022, when the PSC was advised that the project ‘forecasted that it would exceed its agreed budget and schedule tolerances’. In May 2022, the PSC approved re-baselining the schedule (that is, revising the IOC delivery date from October 2022 to 25 November 2022).

3.90 In August 2022, the PSC was advised that the approved Portal to Platform design needed revision due to issues with the stability of applications within Defence’s ICT environment.

Infrastructure outages in the lower environments ... have impacted and are continuing to impact myClearance delivery. At this stage, the delivery of IOC by December to meet Defence’s commitment to Government is at significant risk. In addition, outages post IOC Go Live will likely lead to a poorer customer experience as well as more complexity in sustaining the platform. ...

As a mitigation to the risk of further delay to IOC, an alternative Portal to Platform connectivity is being explored in which the Portal to Platform communication is proposed to be via a different and simplified secure gateway retaining overall benefits of the platform for AGSVA whilst reducing platform stability and delivery risks.

### *Accreditation and security management*

3.91 The myClearance system is a major application within Defence’s ICT environment and is used to collect, communicate, process and store highly sensitive personal information, including psychological assessments. It is then used to inform decisions to grant or deny security clearances. The myClearance system must be accredited and comply with the requirements of the Defence

Security Policy Framework (DSPF)<sup>120</sup> and the Protective Security Policy Framework (PSPF).<sup>121</sup> According to the PSPF, personally identifiable information is classified as OFFICIAL: Sensitive, and in aggregate is classified as PROTECTED.

3.92 The myClearance system operates as follows.

- The Vetting Portal (System of Engagement) is the publicly available and accessible front end of the myClearance system and is hosted in an OFFICIAL cloud environment. It is used to collect information from external users<sup>122</sup>, pass information to AGSVA for processing, and communicate between AGSVA and external users.
- The Vetting Platform (System of Record) is the ‘backend’ of the myClearance system and is hosted in a PROTECTED cloud environment.
- Information is entered into the Vetting Portal, transferred to the Vetting Platform, and stored in the records management module of the myClearance system.

3.93 As part of the build process, the project planned to achieve accreditation of the system in phases. Provisional ICT accreditation (PICTA) was achieved in stages for periods of between six and nine months, to implement the controls and mitigation activities required to reduce the risk rating from its initial rating of ‘high’ to an acceptable rating (as assessed by Defence) of ‘moderate’.

3.94 After myClearance went live on 28 November 2022, a further PICTA was completed, as required, in June 2023 to accredit the changes made to the approved architecture. The changes were required to introduce alternative multi-factor authentication methods for users within Sensitive Compartmented Information Facilities (SCIFs) where personal mobile devices are prohibited (preventing the use of myGovID to authenticate users and grant access to the Vetting Portal).

3.95 During development and at go-live, Defence had incorrectly identified that the system needed to be rated to hold OFFICIAL information, rather than OFFICIAL: Sensitive information. The error was corrected by June 2023, however the Vetting Portal had been processing personal and sensitive data since 28 November 2022.

3.96 The myClearance system is reliant on the underlying controls and accreditation of the Defence Azure PROTECTED and OFFICIAL hubs. The Defence Azure OFFICIAL Hub was not accredited until February 2023 and other Defence systems with which the myClearance system interfaces and/or integrates are operating under provisional accreditation.

3.97 Full accreditation of the myClearance system was provided by Defence in November 2023 for three years.

3.98 Maintaining and supporting ICT systems requires some user accounts, at the network and application levels, to have extensive access rights (privileged access). Privileged user accounts can

---

120 Principle 23 of the DSPF requires that assurance processes and appropriate protections for Official Information during processing, storage and communication are applied to all Information Communications and Technology (ICT) systems and capabilities prior to use.

121 Policy 11 of the PSPF requires that entities must ensure the secure operation of their ICT systems to safeguard their information and data and the continuous delivery of government business by applying the Information Security Manual’s cyber security principles during all stages of the lifecycle of each system.

122 External users include clearance subjects, clearance sponsors, external vetting service providers, psychologists, and security officers.

be used to circumvent security controls to make direct changes to system settings or data, and to access files and accounts used by others. The Information Security Manual (ISM) requires that user accounts should be removed or suspended when there is no longer a legitimate business need for the user to access the system, including when personnel (such as security officers and authorised decision-makers) and other users involved in the clearance process change duties, leave their position, leave the organisation, or are detected undertaking malicious activities (insider threat).

3.99 On these matters, Defence advised the ANAO in December 2023 as follows.

- Defence does not have a program in place to revalidate user access or revoke or suspend access to the myClearance system.
- While the applications of the myClearance system collect and store security logs, Defence does not have a program in place to monitor or review privileged user activity and does not have a process to periodically revalidate user accounts.

3.100 The effective management of user access and privileged user accounts is a requirement of the Information Security Manual (ISM).

## Recommendation no. 2

3.101 The Department of Defence develop and implement a program 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.*

3.102 *Defence will develop and implement a program to 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.*

### Information management — data quality

3.103 The personnel security clearance process requires high quality information for effective decision-making. Inaccurate information and/or data quality issues can affect decisions to grant or deny security clearances. To be migrated effectively from the existing database, the data needed to be cleansed, extracted, and re-structured to fit into the tables of the myClearance database.

3.104 Data quality was consistently identified as a high risk in Defence's data migration planning documentation. An internal data quality assessment of the structured data within the existing PSAMS2 database was conducted. The result of the assessment were included in a data quality report that was issued for approval on 23 October 2020 and endorsed by Defence on 25 November 2020. The data quality assessment identified that of the 796 columns in the database, 456 (57 per cent) contained data quality issues. The report stated that the impact rating for the PSAMS2 data was 'high' and that a 'low' data quality rating was assigned. The report further stated that a substantial remediation effort was required and that failure to resolve these issues would have a 'direct impact' on the data migration process to the new myClearance system.

3.105 A data cleansing plan was developed to clean data before extracting, transferring and loading it into the myClearance system. The plan was developed in June 2021 and responsibility for data cleansing was given to AGSVA. Implementation of the plan was to occur over 12 months, and

approval was given by AGSVA to migrate the data in July 2022. By July 2022, not all data quality issues had been resolved. These unresolved issues were documented in a 'Phase 2' data cleansing plan in July 2022, which identified nine 'data quality items requiring remediation' prior to migration.

3.106 To migrate the data into the new system, three trial migrations were completed between November 2021 and May 2022, and four 'dress rehearsals' were held between June and October 2022. These activities were to: establish an end-to-end migration process; identify data quality issues; and enable retesting.<sup>123</sup> The ANAO identified the following issues with the data cleansing and migration activities.

- The scope of Defence's data cleansing process and quality requirements were not clearly defined in the data cleansing plan.
- Further risks and issues requiring remediation were identified after data cleansing was completed and trial migrations conducted.
- Dress rehearsals were unable to be performed end-to-end as planned due to external system integration issues.
- The data used to conduct testing was not representative of the population. The highest risk data (open cases) was not tested during the trial migration phase as the open case migration build had not been completed in time.
- Defence did not establish formal acceptance processes for the results from the dress rehearsals prior to implementation.

3.107 In May 2022, the Project Steering Committee (PSC) was advised that the project was '[r]eviewing data quality remediation activities and planning with AGSVA for Initial Operating Capability'. In August 2022, the PSC was advised that:

There are numerous known challenges with existing data states that are present in the current vetting database (PSAMS2) that may not migrate effectively into the new myClearance data model.

3.108 The PSC was also advised that the data migration status was 'green' and asked to note the data migration status, challenges and next activities.

3.109 Shortly after the myClearance system went live, at the end of November 2022, these data quality risks and issues were realised. For example, incorrect data was displayed for users that were able to access the system and users were prevented from logging into the system where the information in the system did not match the information in myGovID.

3.110 In January 2024, Defence advised the ANAO that data cleansing was being performed up to 22 November 2022, when the 'Final Migration of data from legacy system [PSAMS2]' was completed. At February 2024, the data quality issues were still being addressed and remediated on a case-by-case basis. In June 2024, Defence confirmed that this case-by-case approach to remediation remains in place and will continue to 'reduce as legacy data is progressively remediated' over time.

---

123 The trial migrations used 'dummy data' for the first trial and masked production data for the other two trials. Dress rehearsals involved more complex preparation for the 'extract, load and transfer' of production data and was intended to test workspace creation and the migration of open cases using unmasked data in an appropriately secure environment.



## Testing

3.111 The Defence Capability Life Cycle Manual (CLC) requires that a Test and Evaluation Master Plan (TEMP) be developed. The TEMP is a core document and is to be updated to reflect changes throughout the acquisition and sustainment phases of a system.

3.112 Defence's ICT Software Testing Manual 2019 also provides guidance on how to conduct testing activities for ICT projects within Defence.

3.113 The September 2020 TEMP for the Vetting Transformation Project stated that a Master Test Plan (MTP) would describe the testing approach and defect management process. Between the execution of the Prime Systems Integrator contract (in February 2021) and March 2024, the MTP was updated nine times, with the most recent version endorsed on 18 May 2023. In November 2023, Defence advised the ANAO that the MTP was used to guide testing activities instead of the TEMP.

3.114 The MTP set out Defence's approach to testing, including: the test types, test phases and related release (IOC/FOC); entry and exit criteria; retesting and regression testing; test deliverables; and work products. Supporting the MTP were individual test plans developed for: Systems Testing; Systems Integration Testing (SIT); Performance Testing; Security Testing; User Acceptance Testing (UAT); Operational Readiness Testing; and Production Verification Testing.<sup>124</sup>

3.115 The key testing phases that were to be completed before launching the system were Systems Integration Testing and User Acceptance Testing. These phases are examined in more detail in the following sections.

### *Systems integration testing*

3.116 Systems Integration Testing (SIT) is a phase that tests the functional requirements and includes validating the interfaces and integration with external and internal systems. It is run in a production-like test environment and should test the process end-to-end to ensure business procedures can be successfully operated in the new system. Defence approved the SIT Test Plan on 3 November 2021. This document detailed the scope of testing, responsibilities, entry and exit criteria, and other key information to guide the SIT phase.

3.117 In October 2021, the IPMT was advised that SIT was at risk due to delays impacting the critical path. In February 2022, the PSC was advised that connectivity issues were blocking the systems testing of the myGov digital identity service and its integration with the Vetting Portal. In May 2022, the PSC was advised that the project had forecasted that it would exceed agreed budget and schedule tolerances and that SIT was not able to commence as scheduled in December 2021 because key elements of the solution (hardware, software and cloud services) to be sourced by Defence had not been delivered on time. The SIT commenced on 4 March 2022 and concluded on 11 November 2022. SIT had not been completed when User Acceptance Testing commenced.

---

124 Testing for the Vetting Transformation Project included functional and non-functional testing. Functional testing included unit testing, usability and accessibility testing, system integration testing, system testing, user acceptance testing, and product verification testing. Non-functional testing included security testing, performance testing, operational readiness testing and high availability testing.

### *User acceptance testing*

3.118 User Acceptance Testing (UAT) is a functional test phase that confirms business requirements are met from the perspective of an end-user. Defence's Test and Evaluation Policy states that ICT test and evaluation is to comply with the Information and Communications Technology (ICT) Software Testing Manual. The completion of UAT is a requirement of the Defence ICT Software Testing Manual. The 2019 ICT Software Testing Manual, in effect at the time of testing for the myClearance system, provides the following guidance.

- User Acceptance Testing (UAT) establishes confidence in the system by assessing the readiness for deployment and complying with end-user requirements from a business and system administration perspective.
- [The] test planning, test preparation, and test reporting for UAT are the responsibility of the solution provider with test execution undertaken by Defence's system end-users.
- UAT will be performed in a production-like test or pre-production environment using real world business scenarios.
- UAT is the joint responsibility of the solution provider and Defence.

3.119 The Test and Evaluation Master Plan (September 2020) stated that resources from AGSVA, industry and other government agencies would be required to assist the project conduct acceptance and operational test and evaluation activities. On 3 June 2022, Defence approved the UAT test plan for the myClearance system. The test plan identified what was being tested, when testing was to occur, who was to be involved and the entry and exit criteria that were to apply.

3.120 The UAT process did not fully accord with the ICT Software Manual or aspects of the UAT test plan (see paragraphs 3.118 to 3.119), with the following shortcomings identified.

- Cleansed and masked data was not used for UAT testing.<sup>125</sup> The data used for UAT was not representative of, or comparable with, production data. The risks associated with not using representative data were identified in September 2022, approximately three months after the UAT Plan was approved. These risks were assessed as 'high' and were to be mitigated by data validation activities that were not overseen by Defence.
- Exit criteria for UAT included having no open severity level one or two defects present<sup>126</sup>, however the assessments were limited to the technical severity and did not assess the business impact of the defect. At 18 November 2022, 90 defects were outstanding. Of these, six were assessed as severity two with five being a priority two and one a priority one. The priority of the defect<sup>127</sup> played no role in the decision to go live.
- Representatives invited to participate in UAT were Defence, the Prime Systems Integrator and external vetting service providers. Representatives from other (partner) entities were not invited to participate. Clearance subjects, security and vetting officers — who needed

---

125 Data for UAT testing was to use production (live) data that had been cleansed and masked to protect inadvertent disclosure to UAT participants who did not have a 'need to know'.

126 The severity rating of the defect relates to the impact of the defect on the software being tested and/or the risk that would occur if the defect was not fixed prior and was released into production. Severity level one indicates the highest level of impact.

127 The priority rating indicates the importance or urgency of fixing the defect.

to access system from outside the Defence Information Environment — were also not included.

3.121 The MTP (October 2022) stated that UAT would not be restricted to AGSVA personnel and should include security officers, sponsoring entities, external security vetting services and psychologists. Participation in testing activities by the full range of anticipated system users would have provided additional assurance to Defence that the system requirements and capability uplift would be delivered.

Assessment of the Remediation Plan for the myClearance System

3.122 In March 2023, Defence commissioned a review to conduct ‘an initial assessment of the remediation plan’ that was developed after the launch of the myClearance system on 28 November 2022.<sup>128</sup> The review found that there were ‘four areas in the remediation plan where work [was] still needed, including the remediation of data.’<sup>129</sup> The review made the following observations on the effectiveness of UAT and Defence’s implementation.

The user acceptance testing clearly failed to expose the problems encountered after go live. It appears to have been rushed, superficial and poorly designed. The design and execution of the UAT would deserve more detailed analysis. One thing is clear: it must be more rigorous going forward. And for the next phase of the project, it should not take place until system design and system integration are finished.

The implementation of a project of this complexity and importance should have been in stages: new Baseline clearances, then all Baseline clearances, then new NV1s ... I listened to the arguments about how that would have complicated the roll-out but the short term pain would have been less than that experienced from the ‘all at once’ implementation attempted. A staged approach to the next phase is essential.

3.123 Defence’s work to remediate the issues experienced after the system went live (on 28 November 2022) is discussed from paragraph 3.135.

### **Delivery of the business need and capability requirements**

3.124 The business need and capability requirements that the project was to deliver were developed during the planning and risk mitigation and requirements setting phases of the project. They are detailed at paragraphs 2.12 to 2.29 and Appendix 4.

#### *Delivery of business needs*

3.125 In December 2020, Defence advised government that the future vetting capability (myClearance) to be delivered by the Vetting Transformation Project would meet the business needs outlined in Table 3.2. An assessment of the extent to which the myClearance system has met the business needs as at May 2024 is outlined in Table 3.2.

---

128 The review was undertaken by Stephen Merchant Consulting. Stephen Merchant was the Deputy Secretary for Intelligence and Security for the Department of Defence from 2006 to 2011.

129 The other three areas were: ‘improvements to enable the seamless transfer of clearance packs between AGSVA and ASIO; enabling a fuller set of business reporting needs to be met; and improving customer service and ensuring a positive experience for those using the system’.

**Table 3.2: Business needs and capability requirements — assessment of delivery**

Business need advised to government in December 2020	ANAO assessment	ANAO comment
Increased efficiency of vetting to reduce processing timeframes for all clearance levels.	Partly met	For 2023–24, 38,490 (55 per cent) of the 71,218 cases have been processed within agreed KPIs. <sup>a</sup> Month on month median processing timeframes for Baseline and Positive Vetting clearance levels have improved and were within KPIs, as at 9 May 2024.
Increased corroboration of information from trusted government and non-government sources to reduce the need for Defence to store some information, and better inform vetting decisions and clearance subject risk profiles.	Not met	This functionality has been removed from the scope of the project.
Improved analysis and sharing of risk information, enabling more effective management of personnel security threats through advanced analytics and continuous assessment.	Not met	The continuous assessment and advanced analytics functionality has been removed from the scope of the project.
A secure vetting system that shares timely information regarding personnel security risks with sponsoring entities.	Not met	The automated risk sharing functionality has been removed from the scope of the project. Risk information is shared by AGSVA using a manual process outside of the myClearance system.
Seamless transfer of information to other government agencies.	Not met	This functionality has been removed from the scope of the project.
Secure system access for industry service providers, negating the need to transport paper files between Defence and industry.	Fully met	The myClearance system eliminated the need to transport paper files between Defence and industry.
Scalability to account for future demand and growing workforce.	Largely met	Changes to the vetting risk model and the internal and external integrations can be made to the system.
Flexibility to adapt to emerging threats and changes in policy.	Partly met	In November 2023, elements that were anticipated to enhance emerging threat intelligence were removed from the scope of the project. Despite this, the new system has increased AGSVA's capability to respond to changes in security priorities.

Note a: In November 2023, AGSVA advised government that 9,795 cases remained over benchmark KPIs, however processing times are steadily reducing.

Source: ANAO analysis of Defence documentation.

3.126 In November 2023, Defence advised government that the project would not be able to deliver the full capability of the system as advised in December 2020, and recommended de-scoping the continuous assessment functionality (module two). Government agreed to the recommendation in November 2023.

3.127 As such, the Vetting Transformation Project (now myClearance) has partly met the business needs identified in the December 2020 Joint Capability Needs Statement and as advised to government.

### *Benefits realisation*

3.128 In December 2020, Defence advised government that the Vetting Transformation Project would deliver the following benefits for government and Australian industry:

- improved detection of security risks and mitigation of the insider threat;
- enhanced customer experience;
- improved ability to meet fluctuations in growing demand;
- reduced operating costs;
- opportunities for extension to all authorised vetting agencies; and
- Australian Industry benefits.

3.129 A Benefits Realisation Plan (BRP) was submitted to the Integrated Project Management Team (IPMT) in August 2021 and was endorsed on 5 May 2022.

3.130 The benefits identified in the BRP mirrored those identified in the Business Case developed in 2020. The plan set out: the measures and metrics that would be used to assess the extent to which the benefit had been realised; the governance and accountability mechanisms, including review and reporting requirements; and established benefit profiles for each measure.

3.131 Under the BRP, the Assistant Secretary, Vetting was responsible for benefits reporting. The BRP stated that baseline values would be determined through the transformation phase of the project, and that benefits reporting to the PSC would commence no later than one month after launching myClearance, with quarterly and annual reporting to follow, see Table 3.3.

**Table 3.3: Benefits realisation reporting requirements**

Reports to	Frequency	Most recent reporting
AGSVA Governance Board	Quarterly	15 August 2023
Project Steering Committee	Monthly	April 2023
Digital Transformation Agency	Quarterly	May 2023
Minister for Defence	Annually	–

Source: ANAO analysis of Defence documentation.

3.132 In August 2023, Defence advised the AGSVA Governance Board that benefits realisation reporting had not commenced due to the need to establish the myClearance remediation taskforce and resolve the system issues encountered after myClearance went live on 28 November 2022 (see paragraph 3.135).

3.133 At January 2024, benefits reporting had only been provided to the DTA. The reporting focused on whether the benefit is able to be realised. The reports examined by the ANAO did not identify the measures or metrics that will be used to assess the extent to which the expected benefits have been or are likely to be realised.

3.134 On the basis of the benefits reporting provided to date, Defence is not able to demonstrate to what extent, if any, the expected benefits have been, or are likely to be realised.

### **myClearance remediation**

3.135 The myClearance system went live on 28 November 2022. By February 2023, the extent of user issues experienced after the launch were the subject of parliamentary interest. Identified deficiencies related to data quality, accessibility, functionality, reporting, and the user interface. The following are examples of identified issues.

- Incorrect data displayed for users, preventing submission of clearance requests and processing actions, requiring remediation.
- Repeated login failures due to credential matching errors between data fields (surname and date of birth) in the myClearance system and myGovID.
- Communication failures and capacity constraints between the myClearance system and its integration/interfaces with systems external to Defence involved in the vetting process, including the Australian Criminal Intelligence Commission (ACIC) to request police checks and referrals to ASIO/AGD to conduct security assessments.
- Weaknesses in the role-based access controls governing the visibility of clearance information, including sensitive personal information.
- Security officers unable to access the myClearance system within secure environments where personal mobile devices required for digital identity authentication purposes (myGovID) are prohibited.
- Incomplete information displaying in cases transferred to ASIO/AGD for processing.
- Business reports not built into the system.
- Customer service and support arrangements overwhelmed, resulting in substantial wait times to respond to and resolve issues.

3.136 In February 2023, a myClearance remediation taskforce was established to monitor the implementation of a remediation plan to rectify the data quality, accessibility, reporting, and interface deficiencies. The taskforce was led by an SES Band 1 official, supported by approximately 80 personnel including representatives from AGSVA and CIOG. The taskforce was dissolved in July 2023.

3.137 Between March and July 2023, the Assistant Minister for Defence was provided with a weekly update on the activities of the remediation taskforce (see paragraph 2.97).

3.138 In October 2023, the Minister for Defence was advised that to address the issues encountered, Defence had done the following.

- Stood up a dedicated remediation taskforce led by a senior executive officer.
- Introduced both technical and data enhancements to enable security clearance applications to progress through the system, including the ability for applicants to edit and delete information.
- Delivered enhancements to myClearance in support of interfaces with the Australian Criminal Intelligence Commission (ACIC) and the Attorney-General's Department (AGD), enabling the majority of cases to progress for external checks without intervention.

- Broadened the testing process to ensure testing occurred on production-like data and with a broad testing cohort.
- Introduced a new log-in solution for security officers, using multi-factor authentication accessible from secure facilities.

3.139 In November 2023 Defence recommended that the government agree to de-scope the following from the myClearance system: continuous assessment; automated risk sharing; use of artificial intelligence; and enhanced interface functionality. As a consequence, the myClearance system will not deliver the full functionality as advised to government in December 2020.

---



Rona Mellor PSM  
Acting Auditor-General

Canberra ACT  
11 July 2024





# Appendices

## Appendix 1 Department of Defence response



Australian Government

Defence

PO Box 7900 CANBERRA BC ACT 2610

EC24-002686

**Ms Rona Mellor, PSM**  
Acting Auditor-General  
PO BOX 707  
CANBERRA ACT 2601

Dear Ms Mellor *Rona*

**Auditor-General Proposed Report – Defence’s procurement and implementation of the myClearance system**

Thank you for the opportunity to comment on the Proposed Report for the Auditor-General performance audit *Defence’s procurement and implementation of the myClearance system*.

Defence acknowledges and accepts the key findings and recommendations made to improve Defence’s management of risk and the security of the myClearance system. Defence is committed to strengthening procurement and governance arrangements, ensuring important projects are delivered in the best interests of Australia’s national security.

Attached to this letter are Defence’s proposed amendments, editorials and comments (**Annex A**), response to requests for information (**Annex B**), response to proposed recommendations (**Annex C**) and Defence’s summary response (**Annex D**). These constitute Defence’s formal response to the Auditor-General Proposed Report.

Our point of contact is the ANAO Liaison Officer who can be contacted via email at: [anao.lo@defence.gov.au](mailto:anao.lo@defence.gov.au).

Yours sincerely

*Greg Moriarty*  
**Greg Moriarty, AO**  
Secretary  
13 June 2024

*Angus J Campbell*  
**Angus J Campbell, AO, DSC**  
General  
Chief of the Defence Force  
13 June 2024

## Appendix 2 Improvements observed by the ANAO

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

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

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

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

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

- Defence stood up the myClearance taskforce in February 2023 to oversee the implementation of a remediation plan to address the issues encountered after the system 'went live' in November 2022. The taskforce was dissolved in July 2023. At March 2024, work to remediate the issues was ongoing (see paragraphs 2.80 and 3.135 to 3.139).
- Defence has agreed to change its approach to deliver major ICT projects from a 'high' risk approach that uses large-scale releases to one that uses major and minor updates and/or releases to add functionality to ICT systems more frequently, in line with recommendations from the Defence Strategic Review (see paragraph 3.67).

## Appendix 3 Vetting Transformation Project budget

1. The tables below (Table A.1 and Table A.2) provide the total acquisition and sustainment budgets for the myClearance system, as approved in December 2020.

**Table A.1: Acquisition budget, as approved by government in December 2020**

Item description	2020–21	2021–22	2022–23	2023–24	Contingency	Total
	\$m	\$m	\$m	\$m	\$m	\$m
Systems integration	20.9	43.4	14.7	–	4.0	83.0
Software	5.1	0.2	–	–	0.3	5.6
Hardware/infrastructure	0.4	1.1	–	–	0.6	2.1
Organisation Change Management	1.2	3.4	3.4	0.3	1.2	9.5
External Agencies Data Integration	2.9	1.1	–	–	0.9	4.9
Integration costs	3.9	4.1	–	–	3.2	11.2
Logistics	–	0.1	–	–	–	0.1
Contractor Support Services	1.3	5.6	4.5	–	1.7	13.1
Other items	1.5	2.2	1.6	0.9	2.9	9.1
<b>Acquisition budget</b>	<b>37.2</b>	<b>61.2</b>	<b>24.2</b>	<b>1.2</b>	<b>14.8</b>	<b>138.6</b>

Source: ANAO analysis of Defence documentation.

**Table A.2: Sustainment budget, as approved by government in December 2020**

Item description	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	Total
	-21	-22	-23	-24	-25	-26	-27	-28	-29	-30	-31	-32	-33	
	\$m	\$m	\$m	\$m	\$m	\$m	\$m	\$m	\$m	\$m	\$m	\$m	\$m	\$m
Systems Integration	–	3.3	7.6	8.0	6.9	8.3	7.9	8.0	8.1	8.3	(4.2)	(4.3)	1.5	59.4
Software	–	–	0.6	0.6	0.6	0.7	0.7	0.7	0.7	0.7	0.7	0.8	0.1	6.9
Hardware	–	1.9	2.6	2.8	2.7	2.8	2.8	3.0	3.0	3.1	3.1	3.3	1.6	32.7
Integration	–	–	1.3	1.6	1.7	1.7	1.7	1.8	1.8	1.9	1.9	2.0	–	17.4
Contractor Support Services	–	–	1.0	1.0	1.0	1.0	1.1	1.1	1.1	1.1	1.2	1.2	–	10.8
Other items	–	–	0.1	0.1	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	–	1.8
Current eVetting sustainment	–	–	1.3	2.1	2.6	0.1	0.6	0.5	0.9	0.8	13.5	13.8	3.3	39.5
Sustainment budget	–	5.2	14.5	16.2	15.7	14.8	15.0	15.4	15.8	16.1	16.4	16.9	6.5	168.6
<b>Total acquisition and sustainment budget</b>	<b>37.2</b>	<b>66.4</b>	<b>38.7</b>	<b>17.4</b>	<b>15.7</b>	<b>14.8</b>	<b>15.0</b>	<b>15.4</b>	<b>15.8</b>	<b>16.1</b>	<b>16.4</b>	<b>16.9</b>	<b>6.5</b>	<b>307.2</b>

Source: ANAO analysis of Defence documentation.

## Appendix 4 Vetting Transformation Project — Business Outcomes

Capability	Description
Efficient and automated business processes	Future vetting processes will support efficient interactions between AGSVA and its customers and data providers, redistribute resources to high-value tasks, and eliminate unnecessary manual and duplicative processes.
Effective information collection and management	<p>The vetting capability will use automated data feeds from source agencies to verify information. Using authoritative sources, such as the Australian Government Document Verification Service, will mitigate risk where the supplied information may be incomplete, inaccurate or deliberately misleading.</p> <p>The capability will provide interoperability and integration with key Defence and Government systems to support efficient and secure transfer of information, including with ASIO, Home Affairs, and ACIC.</p> <p>The capability will enable access to publicly accessible digital footprints, such as social media profiles, to support verification of supplied information and identification of potential insider threats.</p> <p>The capability will also support digitisation, sentencing and destruction of physical personnel security files. Currently AGSVA manages more than 400,000 physical files.</p>
Flexibility, scalability and adaptability	The supporting ICT systems will to the extent practicable, be able to adapt to future growth in the demand for clearances and to changes in threat and policy. The capability will be flexible so that changes can easily be made to risk models and integrations as requirements change over time. The project will deliver a foundational platform for use by Defence, capable of extension to other Australian Government vetting agencies.
Innovative technology that facilitates automation and information sharing	<p>The assessment of capability improvements will include identification of leading technology opportunities that can complement Defence's ICT strategy and other key Australian Government reforms including:</p> <ul style="list-style-type: none"> <li>secure data sharing between Government agencies;</li> <li>automating processes to remove highly manual tasks; and</li> <li>leveraging secure cloud-based and mobile accessible technology to provide a contemporary, more user friendly experience.</li> </ul>
Effective assessment of clearance applicant and holder risk	Through information sharing, advanced analytics, and intelligence reporting, the future vetting capability will continually assess the risk profile of Clearance Applicants and Holders, allocate resources, and share relevant risk information with employing agencies. The level and frequency of assessment will be proportionate to the security clearance level and risk profile of the Clearance Holder.
Support for personnel security policy and legislation	The future capability will provide the interoperability with key information systems in Defence and other Government agencies required to support efficient and secure transfer of information.
Security of vetting information	The vetting capability will protect all vetting information, including Clearance Holder information, risk assessments and clearance decisions from security threats, including cyber security threats, by remaining compliant with relevant policy and legislation. This includes the PSPF, Defence Security Principles Framework and Information Security Manual.

Capability	Description
Enhanced demand and supply data	The vetting capability will be able to use data to inform demand for vetting and the supply of resources and enable AGSVA to manage internal and external workforces to respond accordingly. This will be supported by business intelligence reporting and advanced analytics.
Continuous process improvement	The future vetting system will collect performance data to enable the business to iteratively and incrementally improve efficiency. Key performance indicators will be reviewed to develop more achievable and measurable indicators for effectiveness, efficiency, quality management and customer experience.
Digital data	All records should be in digital form, by default, in support of the Government's Digital by Default Policy. The experience should be seamless, so that customers and users can complete tasks with minimal frustration or barriers.
Self-validation and assessment by Clearance Applicants and Holders	The vetting capability will inform and assist Clearance Applicants and Holders to understand when information is incomplete or inconsistent. It will identify documents that are missing and provide immediate feedback based on failure to meet mandatory criteria.
Cost attribution	The vetting capability will accurately capture and attribute the cost associated with each type of clearance, to inform implementation of a full cost recovery model, inclusive of ASIO services.

Source: Joint Capability Needs Statement for the Vetting Transformation Project.

## Appendix 5 Functional and non-functional requirements of the future vetting capability

**Table A.3: Functional requirements of the myClearance system**

Category	Description
Application management	The ability to apply for clearance, track a clearance application, manage clearance sponsorships and interests and application financials.
Clearance management	The ability to create, manage and administer a clearance record, including management of a clearance applicants and holder's risk profile and clearance levels.
Assessment management	The ability to create, conduct and manage a vetting assessment and risk rating, and collect and validate data for the vetting assessment.
Clearance outcome management	The ability to create and manage clearance recommendations, decisions and outcomes, and conduct a procedural fairness review of a case.
Business process management	The ability to create and manage workflows, tasks, alerts and reminders, allocate and manage work, continuously improve vetting processes, manage service providers, manage user access profiles and permissions and generate and manage reports and information.
Ongoing suitability assessment and reporting	The ability to conduct ongoing suitability assessment, manage risk models, generate notifications and adjust ongoing suitability assessment regimes.

Source: Gate 2 Vetting Operational Model for the Vetting Transformation Project.



**Table A.4: Non-functional requirements of the myClearance system**

Category	Description
Presentation/User experience	The solution will have the ability to provide a consistent look and feel, including colours, layout, and the behaviour of dynamic elements such as forms, buttons, boxes, popups, navigation, menus and errors.
Security	Ability to provide and configure the desired level of security and to protect the system against both voluntary and involuntary corruption.
Data	The system will provide a clear data structure and architecture while ensuring high integrity, security and auditability under prescribed governance rules.
Integration	The system will have the ability to interface and integrate with required systems
General Technical	Requirements for the solution to follow design principles, enable effective and efficient support, maintenance and deployment options.
Infrastructure	The solution will have the ability to work efficiently, effectively and continuously within Defence and Whole of Government environments, and in compliance with associated policies.
Performance	The solution will provide and monitor the capacity required to meet system availability, response time, and service levels for predefined workloads.
Reporting and Compliance	Ability to provide functionality that allows data querying, reporting on data using predefined and customisable report templates and to meet any regulatory and compliance requirements.

Source: Gate 2 Solution design and technical architecture for the Vetting Transformation Project.

## Appendix 6 Project approval and support services contract with Deloitte — Contract Change Proposals (2017 to 2021)

CCP Number	Description	Approval date	Project	Vetting Project \$m	Total increase \$m
1	Updated Statement of Work and contract deliverables to include stakeholder engagement and milestones to achieve Gate 1 for Vetting Transformation and Case Management	5 Apr 17	Both	–	–
2	Invoke extension option for Case Management and Vetting Transformation Projects	24 May 17	Both	2.408	4.772
3	Include new deliverable — Gate 1 program review	12 Oct 17	Both	0.020	0.041
4	Invoke extension option	15 Dec 17	Case	–	9.505
5	Invoke extension option	19 Apr 18	Vetting	11.102	11.102
6	Additional resources to support evaluation activities	4 Sep 18	Both	0.024	0.048
7	Extend procurement team in line with CCP No.4 and No.5	16 Nov 18	Both	–	–
8	Extend procurement team due to delay in issuing the RFQ	6 Jun 19	Both	0.297	0.594
9	Deliver new cost model	6 Jun 19	Vetting	0.086	0.086
10	Additional organisational design and communication services added to the work order	20 Aug 19	Vetting	0.213	0.213
11	Revise dates in line with new schedule, include additional review of documentation	4 Dec 19	Both	0.893	2.141
12	Update work order to reflect agreed changes to milestones and need to resubmit to the Investment Committee	6 Mar 20	Both	–	–
13	Additional Subject Matter Expert support to management	15 Jun 20	Case	–	0.254
14	Additional work package for the provision of subject matter expert to support the proposed operating model, architecture and cyber security requirements	15 Jun 20	Vetting	0.420	0.420
15	Amend subject matter support requirements	25 Sep 20	Case	–	0.168
16	Extend subject matter expert support until November 2020	1 Oct 20	Vetting	0.217	0.217
17	Extend subject matter expert support until December 2020	30 Dec 20	Vetting	0.077	0.077

CCP Number	Description	Approval date	Project	Vetting Project \$m	Total increase \$m
18	Additional work package — continuation of support — acquisition phase — from 11 Jan to 30 Jun 21	5 May 21	Vetting	0.257	0.257
<b>Total</b>				<b>16.014</b>	<b>29.641</b>

Source: ANAO analysis of Defence documentation.