

Delivery of Security Vetting Services Follow-up

Department of Defence

© Commonwealth of Australia 2020

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-609-7 (Print)

ISBN 978-1-76033-611-0 (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 *It's an Honour* website at <https://www.pmc.gov.au/government/its-honour>.

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

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

Or via email:

communication@anao.gov.au





Canberra ACT
7 December 2020

Dear Mr President
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit in the Department of Defence. The report is titled *Delivery of Security Vetting Services Follow-up*. 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

A handwritten signature in black ink, reading 'Grant Hehir'.

Grant Hehir
Auditor-General

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

AUDITING FOR AUSTRALIA

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

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

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

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

Audit team

Ailsa McPherson
Renee Hall
Kim Murray
Nate Wirihana
Song Khor
Sally Ramsey

Contents

Summary and recommendations	7
Background	7
Conclusion	8
Supporting findings	9
Recommendation	10
Department of Defence summary response	10
Key messages from this audit for all Australian Government entities	11
Audit findings	13
1. Background	14
Introduction	14
Previous Auditor-General reports	15
JCPAA Report 479: Australian Government Security Arrangements	16
Rationale for undertaking the audit	16
Audit approach	17
2. Information technology and information security	19
Has Defence implemented JCPAA recommendation 3, to expedite and report back on the ICT2270 Vetting Transformation project?	20
Has Defence implemented JCPAA recommendation 4, to establish extra safeguards and quality control measures to ensure no sensitive data loss?	22
Has Defence implemented the ANAO recommendation contained in the non-public report prepared under subsection 37(5) of the <i>Auditor-General Act 1997</i> ?	28
3. Conditional clearances and sharing of information	32
Has Defence implemented ANAO recommendation 1, to establish operational guidelines for, and make appropriate risk-based use of, conditional clearances?	34
Has Defence implemented ANAO recommendation 2, to obtain explicit informed consent from clearance subjects to share sensitive personal information with sponsoring entities?	36
Has Defence implemented ANAO recommendation 3, to facilitate AGSVA providing sponsoring entities with specific information on security concerns and mitigating factors?	37
Appendices	43
Appendix 1 Department of Defence response	44
Appendix 2 AGSVA delivery of vetting services — data	45
Appendix 3 List of recommendations examined	48
Appendix 4 Project status — ICT2270	50



Audit snapshot

Auditor-General Report No.21 2020–21

Delivery of Security Vetting Services Follow-up



Why did we do this audit?

- ▶ The appropriate and timely implementation of recommendations made to an entity is an important part of realising the full benefit of an audit or parliamentary enquiry, and for demonstrating accountability to the Parliament.
- ▶ The ANAO and Parliament's Joint Committee of Public Accounts and Audit (JCPAA) made recommendations in 2018 and 2019 to Defence to improve the effectiveness of the Australian Government's personnel security arrangements.
- ▶ The audit assessed whether the recommendations made to Defence had been implemented in a timely manner.



What did we find?

- ▶ Of the six recommendations examined in this audit, Defence has implemented four and partly implemented two.
- ▶ In respect to the two JCPAA recommendations and one ANAO recommendation made to improve Defence's security vetting information technology and information security, Defence has implemented one JCPAA recommendation, partly implemented the second and partly implemented the ANAO recommendation.
- ▶ Defence has implemented the three ANAO recommendations relating to improved processes for conditional clearances and information sharing.



Key facts

- ▶ Security clearances aim to provide additional assurance to the employing entity of the suitability and integrity of personnel.
- ▶ The Australian Government Security Vetting Agency (AGSVA, a branch in Defence) was established in 2010 to centrally administer personnel security vetting on behalf of the majority of Australian Government entities.
- ▶ In 2019–20 AGSVA completed 49,425 security clearances.
- ▶ As at 1 July 2020, AGSVA maintained 403,888 active security clearances.



What did we recommend?

- ▶ The Auditor-General made one recommendation to Defence to improve reporting provided to the AGSVA Governance Board about Defence's management of risk to the eVetting system.
- ▶ Defence agreed to the recommendation.

1 out of 2

JCPAA recommendations implemented by Defence.

3 out of 4

ANAO recommendations implemented by Defence.

Summary and recommendations

Background

1. The Australian Government's Protective Security Policy Framework (PSPF) assists Australian Government entities to protect its people, information and assets.¹ In accordance with the PSPF requirements, the majority of entities must use the Australian Government Security Vetting Agency (AGSVA) to conduct security vetting.² AGSVA, a branch within the Department of Defence (Defence), was established in 2010 to centrally administer personnel security vetting on behalf of the majority of Australian Government entities.³

2. In 2017–18, the ANAO assessed the effectiveness of the Australian Government's personnel security arrangements for mitigating insider threats. In Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security* the ANAO made three recommendations to Defence. In accordance with paragraph 37(1)(a) of the *Auditor-General Act 1997* (Cth) (the Act), the Auditor-General determined to omit particular information, including an additional recommendation to Defence, from the public report. A report including this omitted information and the additional recommendation was prepared and a copy was provided to the Prime Minister, Attorney-General, Minister for Defence, Minister for Finance and Minister for Home Affairs, under paragraph 37(5)(b) of the Act.⁴ Defence agreed to implement all four recommendations.

3. In 2018–19, the Parliament's Joint Committee of Public Accounts and Audit (JCPAA) conducted an inquiry into Australian Government security arrangements based, in part, on Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security*. In the report from that inquiry, the JCPAA made three recommendations to Defence. The department agreed with qualification to implement the first recommendation, agreed to implement the second recommendation and did not agree to implement the third recommendation.

Rationale for undertaking the audit

4. Reports of parliamentary committees and the Auditor-General identify risks to the successful delivery of outcomes and areas where administrative or other improvements can be made. The appropriate and timely implementation of agreed recommendations is an important

1 Attorney-General's Department, *The Protective Security Framework* [Internet], AGD, available from <https://www.protectivesecurity.gov.au/> [accessed 30 August 2020].

2 There are six authorised vetting agencies which can issue security clearances for their own personnel. They are the: Australian Federal Police; Australian Secret Intelligence Service; Australian Security Intelligence Organisation; Office of National Intelligence; Department of Foreign Affairs and Trade (DFAT is authorised to issue security clearances at the Baseline, NV1 and NV2 levels) and the Australian Securities and Investments Commission (ASIC is authorised to issue security clearances at the Baseline level only).

3 Department of Defence, *Australian Government Security Vetting Agency* [Internet], available from <https://www1.defence.gov.au/security/clearances> [accessed 30 August 2020].

4 Subsection 37(3) of the Act provides that the Auditor-General cannot be required, and is not permitted, to disclose to: (a) a House of the Parliament; or (b) a member of a House of the Parliament; or (c) a committee of a House of the Parliament or a joint committee of both Houses of the Parliament; information that that has been omitted from a public report on the basis of subsection 37(1).

part of realising the full benefit of an audit or parliamentary inquiry, and for demonstrating accountability to the Parliament.

5. Auditor-General reports released in June 2015 (Auditor-General Report No. 45 2014–15 *Central Administration of Security Vetting*) and May 2018 (Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security*) identified ongoing deficiencies in AGSVA's performance and made recommendations to improve the effectiveness of the Australian Government's personnel security arrangements. Similarly, in April 2019 the JCPAA made recommendations to Defence to improve AGSVA's effectiveness. This audit will provide assurance that recommendations made by the Auditor-General in 2018 and by the JCPAA in 2019 have been implemented in a timely manner.

6. This audit was identified as a JCPAA priority for 2020–21.

Audit objective and criteria

7. The audit objective was to examine the Department of Defence's implementation of agreed recommendations made in Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security* and the related report provided to ministers under subsection 37(5) of the *Auditor-General Act 1997*, and by the Parliament's Joint Committee of Public Accounts and Audit in Report 479: *Australian Government Security Arrangements*.

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

- Has Defence implemented the ANAO and JCPAA recommendations to improve information technology and information security?
- Has Defence implemented the ANAO recommendations to establish and make use of conditional clearances, and to share sensitive personal information with sponsoring entities?

9. The ANAO reviewed Defence's implementation of two JCPAA recommendations and four ANAO recommendations.

Conclusion

10. Of the six recommendations made to Defence by the JCPAA and ANAO, Defence has implemented four recommendations and partly implemented two recommendations.

11. In respect to the two JCPAA recommendations and one ANAO recommendation contained in the non-public Auditor-General report that were made to improve Defence's security vetting information technology and information security, Defence has: implemented one JCPAA recommendation, partly implemented the second JCPAA recommendation, and partly implemented the ANAO recommendation.

12. Defence has implemented the three ANAO recommendations relating to improved processes for conditional clearances and information sharing.

Supporting findings

13. Defence implemented the two non-substantive elements of JCPAA recommendation 3 that it agreed to. Defence agreed to implement the recommendation with qualification, meaning that it did not agree to implement the first, substantive, component of the recommendation, namely to expedite the Vetting Transformation project (ICT2270). Defence agreed to implement the two process components of the recommendation, involving a progress report and updated timeline on the project, which it provided in its response to the JCPAA on 23 August 2019. Defence did not have an established enterprise governance process to monitor its implementation of JCPAA recommendations.

14. Defence has partly implemented JCPAA recommendation 4, relating to the avoidance of sensitive data loss. Defence reported to the JCPAA in August 2019 that it had put in place five measures over the previous 12 months to strengthen the security of vetting information. Implementation of two of these measures has not concluded. Defence did not assess the effectiveness of existing safeguards and quality control measures prior to reporting to the JCPAA. The risk of sensitive data loss was realised in April 2020 when a paper-based personnel security file was lost during transit. Additionally, sensitive information was mishandled when a package containing two paper-based personnel security files was not received by the intended recipient in December 2019. The package had to be opened by the courier firm to identify the intended recipient.

15. Defence has partly implemented the recommendation contained in the non-public Auditor-General report provided to the Prime Minister and Ministers. In June 2018, the AGSVA Governance Board was advised that the recommendation had been completed. Defence continued to undertake remediation activities but no further reporting on the progress of remediation activities was provided to the Board. A range of remediation measures were agreed following Defence's assessment that the eVetting system's residual risk rating was 'high' in November 2018. In addition, a life of type extension (LOTE) was agreed and this is subject to continual review of the system. As of September 2020, risk mitigation activities set out in the LOTE had not been completed and reporting on the management of risk to senior whole of government committees, as specified in the LOTE, had not been undertaken. There has been system monitoring and reporting activity internal to Defence.

16. Defence has implemented ANAO recommendation 1, relating to risk-based clearance requirements. In consultation with the Attorney-General's Department, Defence developed operational guidelines to guide the issuing of conditional clearances. The Vetting Risk Model (VRM) guides vetting officers through the risk factor areas requiring consideration under the Australian Government's Protective Security Policy Framework. Defence's closure of the recommendation in April 2020 was premature as not all contracted vetting officers had completed the necessary training at this time and therefore were not using the VRM. Defence's advice to the AGSVA Governance Board and the Defence Audit and Risk Committee to close the recommendation did not clearly state the expected completion date of training.

17. Defence has implemented ANAO recommendation 2, relating to obtaining explicit informed consent from clearance subjects for information sharing. A revised Security Clearance Informed Consent form was introduced from July 2018, as planned. A signed form is a requirement for a security clearance application to be processed.

18. Defence has implemented ANAO recommendation 3, relating to the provision of information to sponsoring entities. A framework to facilitate Defence providing sponsoring entities with specific information on security concerns and mitigating factors identified through the vetting process was established in October 2019. Implementation of the framework is occurring through a phased approach. Full implementation is expected after the Vetting Transformation project (ICT2270) achieves initial operating capability, which is scheduled for Q4 2022 but remains subject to government consideration.

Recommendation

Recommendation no.1 Paragraph 2.40

That the Department of Defence supports the Australian Government Security Vetting Agency Governance Board fulfil its terms of reference by reporting to the Board on the management of risk in the eVetting system.

Department of Defence response: *Agreed.*

Department of Defence summary response

19. Defence's summary response is provided below. The department's full response can be found at Appendix 1.

Defence welcomes the ANAO Performance Audit Report into the Delivery of Security Vetting Services Follow-up and notes the finding that Defence has implemented four and partly implemented two of the ANAO and JCPAA recommendations examined by the audit.

Defence safely handles more than 40,000 personnel file movements annually as a part of delivering responsive and assured vetting services for Government and Industry. The report documents a range of measures Defence has implemented since 2018 to safeguard information and ensure quality control, including an active accreditation and assurance program for external security vetting providers to meet Defence and Government security requirements.

Defence continues to prepare for modernisation under the Vetting Transformation Project, which is still subject to Government consideration. Defence is committed to continuous improvement and is closely examining the report findings related to these measures. Defence takes seriously the oversight of these complex activities and is taking steps to further strengthen the governance of risk and implement the Auditor General's recommendation.

Key messages from this audit for all Australian Government entities

20. 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

- The provision of accurate and timely information on risk management supports the effective oversight of complex activities by governance committees.
- The audit committee can provide valuable assurance to the accountable authority on the implementation of external recommendations, if enabled by the committee charter.
- Agreeing to implement a recommendation means that the entity acknowledges things can be improved. Entities should not agree to recommendations ‘with qualification’ or ‘in principle’ when the effect of such a response is to disagree or not implement the substance of a recommendation. Implementing a recommendation in its entirety will assist the entity to realise the full intent of the recommendation.

Audit findings

1. Background

Introduction

1.1 The Australian Government's Protective Security Policy Framework (PSPF) assists Australian Government entities to protect its people, information and assets.⁵ There are 16 mandatory core requirements in the PSPF, three of which concern personnel security. These three requirements are intended to facilitate the sharing of Australian Government resources and to mitigate the threat posed by trusted insiders.⁶

1.2 To implement the three personnel security requirements, the entity must:

- ensure the eligibility and suitability of personnel who have access to Australian Government resources, and use the Australian Government Security Vetting Agency (AGSVA) to conduct vetting, or where authorised, conduct security vetting, in a manner consistent with the Personnel Security Vetting Standards;
- assess and manage the ongoing suitability of its personnel and share relevant information of security concern, where appropriate; and
- ensure separating personnel have had their access to Australian Government resources withdrawn and are informed of any ongoing security obligations.⁷

1.3 The PSPF states that entities may use security clearances:

...where they need additional assurance of the suitability and integrity of personnel. This could be for access to security classified information, or to provide greater assurance for designated positions.⁸

1.4 In accordance with PSPF requirements, an authorised vetting agency must assess the clearance subject's suitability to hold a security clearance, and any doubt must be resolved in the public interest.

The Australian Government Security Vetting Agency

1.5 AGSVA was established in 2010 to centrally administer personnel security vetting on behalf of the majority of Australian Government entities. It is a branch within the Department of Defence (Defence) led by the Assistant Secretary Vetting (Senior Executive Service Band 1).

1.6 Defence delivers AGSVA's services through an allocation of 275 full-time equivalent Australian Public Service (APS) staff located across Australia. The majority (92 per cent) of security clearances are processed by external vetting providers.⁹ Defence contracts six external vetting

5 Attorney-General's Department, *The Protective Security Framework* [Internet], AGD, available from <https://www.protectivesecurity.gov.au/> [accessed 30 August 2020].

6 *ibid.*

7 *ibid.*

8 *ibid.* The PSPF details four levels of security clearances: Baseline; Negative Vetting 1 (NV1); Negative Vetting 2 (NV2) and Positive Vetting (PV).

9 Defence internal reporting shows that, as at 30 June 2020, external vetting providers processed 91 per cent of baseline clearances; 95 per cent of Negative Vetting 1 clearances; 95 per cent of Negative Vetting 2 clearances; and 81 per cent of Positive Vetting clearances.

providers, who, through a mix of employees (40 per cent) and sub-contractors (60 per cent), support the clearance process by preparing vetting assessments. Defence APS staff are responsible for making all security clearance decisions including procedural fairness processes.

1.7 In 2019–20 AGSVA completed 49,425 security clearances, including 3,327 positive vetting clearances. As at 1 July 2020, AGSVA maintained 403,888 active clearances.¹⁰ Appendix 2 of this report contains further data on AGSVA’s performance.

1.8 Defence expenditure on AGSVA services for 2019–20 was \$83.26 million.

Previous Auditor-General reports

1.9 Since AGSVA was established in 2010, the Australian National Audit Office (ANAO) has conducted two performance audits of personnel security arrangements, as effective arrangements underpin the protection of the Australian Government’s people, information and assets.

- Auditor-General Report No. 45 2014–15 *Central Administration of Security Vetting* assessed whether Defence provides an efficient and effective security vetting service through AGSVA, and concluded that:

The performance of AGSVA has been mixed, and key Australian Government expectations relating to improved efficiency and cost savings have not been realised.¹¹

- Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security* assessed the effectiveness of the Australian Government’s personnel security arrangements for mitigating insider threats, and concluded that:

AGSVA’s security vetting services do not effectively mitigate the Government’s exposure to insider threats.¹²

1.10 In the most recent report the ANAO made seven recommendations, three of which were directed to Defence.¹³ The ANAO recommended that Defence establish and make use of conditional clearances, obtain explicit informed consent from clearance subjects to share sensitive personal information with sponsoring entities, and develop a framework to enable AGSVA to share sensitive personal information with sponsoring entities.¹⁴

1.11 Further, the Auditor-General determined to omit particular information from the most recent report — in accordance with paragraph 37(1)(a) of the *Auditor-General Act 1997* (the Act) — including an additional recommendation to Defence. A report including this omitted information and the additional recommendation was prepared and a copy was provided to the Prime Minister,

10 Once a security clearance is granted, there are responsibilities for security clearance holders and sponsors to maintain the clearance.

11 Auditor-General Report No.45 2014–15 *Central Administration of Security Vetting*, p.16.

12 Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security*, p.8.

13 Two of the three recommendations were also directed to the Attorney-General’s Department in recognition of the policy responsibilities of the department.

14 Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security*, paragraphs 2.24; 2.37; and 2.47.

Attorney-General, Minister for Defence, Minister for Finance and Minister for Home Affairs, under paragraph 37(5)(b) of the Act.¹⁵

1.12 Defence agreed to implement all four recommendations. The recommendations are detailed in full, with Defence's response, at Appendix 3 of this audit report.

JCPAA Report 479: Australian Government Security Arrangements

1.13 The Parliament's Joint Committee of Public Accounts and Audit (JCPAA) conducted an inquiry into Australian Government Security Arrangements based on the following ANAO reports:

- Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security*.
- Auditor-General Report No. 43 2017–18 *Domestic Passenger Screening — Follow-Up*.

1.14 In April 2019, the JCPAA made three recommendations to Defence:

- expedite the Vetting Transformation project;
- establish extra safeguards and quality control measures to ensure no incidents of sensitive data loss prior to operational capacity of the new vetting system; and
- prepare a full business case to consider the current and alternative service delivery models.¹⁶

1.15 Defence agreed with qualification to implement the first recommendation, agreed to implement the second recommendation and did not agree to implement the third recommendation. The recommendations are detailed in full, with Defence's response, at Appendix 3 of this audit report.

Rationale for undertaking the audit

1.16 Reports of parliamentary committees and the Auditor-General identify risks to the successful delivery of outcomes and areas where administrative or other improvements can be made. The appropriate and timely implementation of agreed recommendations is an important part of realising the full benefit of an audit or parliamentary inquiry, and for demonstrating accountability to the Parliament.¹⁷

1.17 Auditor-General reports released in June 2015 (Auditor-General Report No. 45 2014–15 *Central Administration of Security Vetting*) and May 2018 (Auditor-General Report No. 38

15 Subsection 37(3) of the Act provides that the Auditor-General cannot be required, and is not permitted, to disclose to: (a) a House of the Parliament; or (b) a member of a House of the Parliament; or (c) a committee of a House of the Parliament or a joint committee of both Houses of the Parliament; information that has been omitted from a public report on the basis of subsection 37(1).

16 Joint Committee of Public Accounts and Audit, *Report 479: Australian Government Security Arrangements*, Commonwealth of Australia, 2019, paragraphs 2.33 and 2.43.

17 The ANAO's work program includes a series of performance audits on the implementation of recommendations made by Parliament and the ANAO. The reports published to date are: Auditor-General Report No.6 2019–20 *Implementation of ANAO and Parliamentary Committee Recommendations*; and Auditor-General Report No.46 2019–20 *Implementation of ANAO and Parliamentary Committee Recommendations — Education and Health Portfolios*. A further audit in this series, focusing on Defence's implementation of recommendations, is forthcoming. The ANAO has also drawn together audit insights on the implementation of recommendations at: www.anao.gov.au/work/audit-insights/implementation-recommendations.

2017–18 *Mitigating Insider Threats through Personnel Security*) identified ongoing deficiencies in AGSVA's performance and made recommendations to improve the effectiveness of the Australian Government's personnel security arrangements. Similarly, in April 2019 the Joint Committee of Public Accounts and Audit made recommendations to Defence to improve AGSVA's effectiveness. This audit will provide assurance that recommendations made by the Auditor-General in 2018 and by the JCPAA in 2019 have been implemented in a timely manner.

1.18 This audit was identified as a JCPAA priority for 2020–21.

Audit approach

Audit objective, criteria and scope

1.19 The audit objective was to examine the Department of Defence's implementation of agreed recommendations made in Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security* and the related report provided to ministers under subsection 37(5) of the *Auditor-General Act 1997*, and by the Parliament's Joint Committee of Public Accounts and Audit in Report 479: *Australian Government Security Arrangements*.

1.20 To form a conclusion against the audit objective, the following high level audit criteria were adopted:

- Has Defence implemented the ANAO and JCPAA recommendations to improve information technology and information security?
- Has Defence implemented the ANAO recommendations to establish and make use of conditional clearances, and to share sensitive personal information with sponsoring entities?

1.21 The ANAO reviewed Defence's implementation of two JCPAA recommendations and four ANAO recommendations.

1.22 For two of the three recommendations directed to Defence in Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security*, the recommendation was also directed to the Attorney-General's Department. While the Attorney-General's Department was not designated for this audit, the actions it took to revise personnel security policy requirements were considered. The audit focused on evidence of Defence incorporating these policy changes into the administration of security vetting services to implement the ANAO recommendations.

1.23 Recommendations made in Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security* to entities other than Defence were not in scope for this audit.¹⁸

Audit methodology

1.24 The audit methodology involved:

- examination and analysis of relevant documentation held by Defence;
- demonstration of certain AGSVA business processes;

18 The previous audit included recommendations directed to the Attorney-General's Department, Digital Transformation Agency, Australian Securities and Investments Commission, Department of Home Affairs, and Australian Radiation Protection and Nuclear Safety Authority.

- analysis of data extracted from AGSVA’s security vetting case management system; and
- discussions with relevant departmental staff.

1.25 The audit was conducted in accordance with the ANAO Auditing Standards at a cost to the ANAO of approximately \$341,000.

1.26 The audit team was Ailsa McPherson, Renee Hall, Kim Murray, Nate Wirihana, Song Khor and Sally Ramsey.

2. Information technology and information security

Areas examined

This chapter examines Defence's implementation of two recommendations made by the Parliament's Joint Committee of Public Accounts and Audit (JCPAA) — to expedite Defence's ICT2270 Vetting Transformation project, and to establish extra safeguards and quality control measures to ensure no incidents of sensitive data loss prior to operational capability of ICT2270.

Defence's implementation of the recommendation contained in the non-public Auditor-General report prepared under subsection 37(5) of the *Auditor-General Act 1997* is also examined.

Conclusion

In respect to the two JCPAA recommendations and one ANAO recommendation contained in the non-public Auditor-General report, that were made to improve Defence's security vetting information technology and information security, Defence has: implemented one JCPAA recommendation, partly implemented the second JCPAA recommendation, and partly implemented the ANAO recommendation.

Recommendation

The ANAO made one recommendation aimed at ensuring that the Australian Government Security Vetting Services Agency (AGSVA) Governance Board can fulfil its Terms of Reference by receiving Defence reports on the management of risk in the eVetting system.

2.1 In April 2019, the Parliament's Joint Committee of Public Accounts and Audit (JCPAA) completed its inquiry into Australian Government Security Arrangements, based on Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security* and Auditor-General Report No. 43 2017–18 *Domestic Passenger Screening — Follow-up*.

2.2 In Report No. 479: *Australian Government Security Arrangements*, the JCPAA directed three recommendations to Defence concerning security vetting services (recommendations 3, 4 and 5). Defence agreed with qualification to implement recommendation 3, agreed to implement recommendation 4, and did not agree to implement recommendation 5.¹⁹ This chapter examines Defence's implementation of JCPAA recommendations 3 and 4, which specifically relate to the information systems supporting security vetting services and the potential loss of sensitive personal data (see Table 2.1 below).

2.3 In the context of Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security*, the ANAO conducted work in relation to the security of clearance records. The Auditor-General determined to omit particular information on this matter, including an additional recommendation agreed by Defence, from the public audit report. A non-public Auditor-General report that included the omitted information and additional recommendation was prepared and a

19 Defence did not agree to JCPAA recommendation 5 – that 'Defence prepare a full business case to consider the current and alternative service delivery models, taking account of projected future demand for vetting, the costs, benefits and risks of various approaches, and provide the findings of this to the Committee within 12 months'.

copy was provided to the Prime Minister, Attorney-General, Minister for Defence, Minister for Finance and Minister for Home Affairs under paragraph 37(5)(b) of the *Auditor-General Act 1997*.

2.4 Table 2.1 sets out the three recommendations that Defence agreed to implement in full or with qualification, Defence’s assessment of the status of the recommendation and the ANAO’s summary assessment of Defence’s implementation of the recommendation. In summary, Defence has implemented one recommendation and partly implemented two recommendations.

Table 2.1: Assessment of Defence’s implementation of JCPAA recommendations and the ANAO recommendation contained in the non-public Auditor-General report

Recommendation	Defence assessment	ANAO assessment
<p>JCPAA recommendation 3: Defence expedite the ICT2270 Vetting Transformation project and provide to the Committee a progress report and updated timeline on implementation of the replacement ICT system.</p>	<p>Defence agreed with qualification, noting timing of implementation is subject to Defence project governance review and government approval.</p> <p>Defence reported to JCPAA on 23 August 2019 with a progress report and timeline, noting delay to initial operating capability but reporting ICT2270 is on track for final operating capability in 2023.</p> <p>Defence has not assessed the recommendation as implemented or not.</p>	<p>Defence has implemented the two process elements of JCPAA recommendation 3 that it agreed to, relating to the progress report and updated implementation timeline.</p> <p>Defence agreed to implement the recommendation with qualification, meaning that it did not agree to implement the first, substantive, component of the recommendation, to expedite the Vetting Transformation project.</p> <p>See paragraphs 2.5 to 2.10 of this audit.</p>
<p>JCPAA recommendation 4: Defence establish extra safeguards and quality control measures to ensure that no incidents of sensitive data loss occur prior to operational capability of the new vetting case management system.</p>	<p>Defence reported to JCPAA on 23 August 2019 on activities undertaken by Defence to prevent sensitive data loss.</p> <p>Defence has not assessed the recommendation as implemented or not.</p>	<p>Defence has partly implemented this recommendation.</p> <p>See paragraphs 2.11 to 2.32 of this audit.</p>
<p>ANAO recommendation: Recommendation contained in the non-public Auditor-General report.</p>	<p>Implemented.</p> <p>Recommendation closed on 9 July 2018.</p>	<p>Defence has partly implemented this recommendation.</p> <p>See paragraphs 2.33 to 2.50 of this audit.</p>

Source: ANAO analysis of departmental documentation.

Has Defence implemented JCPAA recommendation 3, to expedite and report back on the ICT2270 Vetting Transformation project?

Defence implemented the two non-substantive elements of JCPAA recommendation 3 that it agreed to. Defence agreed to implement the recommendation with qualification, meaning that it did not agree to implement the first, substantive, component of the recommendation, namely to expedite the Vetting Transformation project (ICT2270). Defence agreed to implement the two process components of the recommendation, involving a progress report and updated timeline on the project, which it provided in its response to the JCPAA on

23 August 2019. Defence did not have an established enterprise governance process to monitor its implementation of JCPAA recommendations.

2.5 The JCPAA recommendation (recommendation 3) contained three components:

- expedite the ICT2270 Vetting Transformation project;
- provide the committee with a progress report; and
- provide the committee with an updated timeline on the project.

2.6 To assess Defence's implementation, the ANAO examined whether Defence had implemented the recommendation in accordance with its qualified response to the JCPAA. On 23 August 2019, Defence agreed with qualification to implement the recommendation, noting that:

Timings of the implementation of the ICT2270 Vetting Transformation project is subject to Defence project governance review and government approval.²⁰

2.7 Defence's response to the JCPAA did not include an undertaking to expedite the project. The response did however provide the committee with a progress report and a broad timeline for achieving final operating capability (FOC) for ICT2270 in 2023 (thereby addressing components 2 and 3 of the recommendation). Defence's response also noted a delay to achieving initial operating capability (IOC) due to the delivery of ICT2270 being managed in line with delivery of a Defence-wide case management system, and another related program of work to update Defence's enterprise SAP systems. Defence's response to the JCPAA advised that ICT2270 was on track to achieve final operating capability in 2023.

2.8 Since Defence responded to the JCPAA on 23 August 2019, there have been further delays to the IOC delivery date for ICT2270. Additional information on the project's status is provided at Appendix 4.

2.9 Defence did not develop an implementation plan for this recommendation, and prior to responding to the JCPAA, did not review options to expedite the project (which was the first component of the JCPAA recommendation, as discussed in paragraph 2.5). Defence's response to the JCPAA addressed the second and third components of the recommendation.

2.10 In advice to the ANAO, Defence confirmed that at this time it did not have an established enterprise governance process to record and monitor the implementation of Parliamentary recommendations.²¹

20 Parliament of Australia, *Report 479 Australian Government Security Arrangements Government Response* [Internet], available from https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/PersonnelSecurity/Government_Response [accessed 15 September 2020].

21 In July 2020, the Defence Audit and Risk Committee proposed an update to the committee charter to include the monitoring and reporting of parliamentary recommendations to the committee. This was approved by the Secretary and Chief of the Defence Force on 17 August 2020. The ANAO is currently examining whether Defence has appropriate arrangements in place to respond to, monitor and implement ANAO and Parliamentary recommendations in a separate performance audit.

Has Defence implemented JCPAA recommendation 4, to establish extra safeguards and quality control measures to ensure no sensitive data loss?

Defence has partly implemented JCPAA recommendation 4, relating to the avoidance of sensitive data loss. Defence reported to the JCPAA in August 2019 that it had put in place five measures over the previous 12 months to strengthen the security of vetting information. Implementation of two of these measures has not concluded. Defence did not assess the effectiveness of existing safeguards and quality control measures prior to reporting to the JCPAA. The risk of sensitive data loss was realised in April 2020 when a paper-based personnel security file was lost during transit. Additionally, sensitive information was mishandled when a package containing two paper-based personnel security files was not received by the intended recipient in December 2019. The package was opened by the courier firm to identify the intended recipient.

2.11 Defence agreed to implement JCPAA recommendation 4. Defence’s response to the JCPAA (dated 23 August 2019) detailed that Defence had put in place five additional measures over the previous 12 months to strengthen security around vetting information.

2.12 Defence did not develop an implementation plan for this recommendation, and prior to responding to the JCPAA, did not: assess the effectiveness of existing safeguards and quality control measures in place to identify what extra safeguards and quality control measures were needed; or document a rationale for the additional measures to show a ‘line-of sight’ between the measure and how the risk of sensitive data loss was reduced by implementing the measure.

2.13 The ANAO’s assessment of the implementation status for the five additional measures advised in Defence’s response to the JCPAA is presented in Table 2.2.

Table 2.2: ANAO assessment of Defence’s additional measures to strengthen security for vetting information

Measure	ANAO assessment of implementation status
In 2018, completed a vetting system remediation program that enhanced ICT security controls.	Partly implemented. Defence enhanced ICT security controls in 2018, and continues to implement risk remediation treatments.
In April 2019, Defence also strengthened Defence Industry Security Program (DISP) requirements.	DISP memberships for external vetting providers (six providers and 117 sub-contractors) are still being completed by Defence.
DISP security requirements are reinforced by the recently established Defence Industry Security Office (DISO) which has responsibility for assuring DISP members’ compliance. DISO conducts reviews and audits of DISP members (including vetting industry members) to ensure appropriate security policies, systems and compliance regimes are in place.	Ongoing.

Measure	ANAO assessment of implementation status
AGSVA is prioritising resourcing to increase External Security Vetting Service panel support staffing to create a new position focused on ICT security assurance.	Implemented. AGSVA has created an Australian Public Service Level 5 (APS5) position with responsibilities that include: ...supporting AGSVA's industry partners to achieve and maintain compliance with Commonwealth and Defence security policy requirements, including membership of DISP.
AGSVA has undertaken a recent refresh of its external security vetting services panel, replacing the previous industry vetting panel. The new panel arrangements commenced on 12 August 2019 and include increased security, professionalisation and capacity standards by requiring panel members to have a national vetting footprint and have all their vetting staff meet AGSVA-directed training competencies.	Implemented. A requirement that the contractor must have all vetting staff meet all AGSVA directed training competencies is contained in the 2019 external security vetting services contract. A requirement for panel members to have a national vetting footprint is contained in the 2019 external security vetting services contract.

Source: Joint Committee of Public Accounts and Audit, *Government Response* [Internet], Parliament of Australia, available from https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/Personnel_Security/Government_Response [accessed 6 September 2020].

2.14 As shown in Table 2.2 implementation is not yet completed in respect to: Defence Industry Security Program (DISP) memberships for external vetting providers and sub-contractors under the strengthened requirements; and DISO assurance activities for DISP members' compliance.

Requirements for external vetting providers to obtain and maintain Defence Industry Security Program membership

2.15 Defence requires all external vetting providers and sub-contractors to obtain and maintain DISP membership.²² The DISP sets minimum security standards required for industry to partner on projects at the 'OFFICIAL', 'OFFICIAL: Sensitive', 'PROTECTED', 'SECRET' and 'TOP SECRET' levels. To attain and maintain DISP membership, entities must meet the DISP eligibility and suitability requirements.²³ To be granted DISP membership, the applicant must meet minimum requirements for governance, personnel security, physical security and information/cyber security. Defence assesses submitted membership applications to confirm eligibility and determine suitability.²⁴

2.16 At the direction of the Australian Government, Defence established the Defence Industry Security Office (DISO) in December 2018, in response to a cybersecurity breach of a Defence

22 This was also a requirement under contractual arrangements prior to Defence's August 2019 refresh of its security vetting provider panel. The six prime contractors are responsible for ensuring their subcontractors apply for, and maintain, DISP membership. Defence's First Assistant Secretary Security and Vetting Services (SES Band 2) is responsible for approving DISP membership.

23 The DISP eligibility and suitability requirements are documented in Control 16.1 of the Defence Security Principles Framework. Department of Defence, *Defence Security Principles Framework* [Internet], available from <https://www.defence.gov.au/dsvs/Master/resources/DSPF-Unclass-Version.pdf> [accessed 7 September 2020].

24 Control 16.1 paragraph 16 of the Defence Security Principles Framework.

contractor in 2018. DISO's primary function is to assess how well companies are meeting their DISP membership security obligations.²⁵

2.17 Defence maintains an excel spreadsheet (register) used to track DISP membership application requirements and assurance activities.²⁶

Assurance activities of DISP membership requirements for external vetting providers

2.18 Defence has undertaken the following assurance activities of DISP membership requirements for the six (prime) external vetting providers and the 117 sub-contractors listed in Defence's tracking spreadsheet.

Sampling assessments

2.19 In July and August 2020, Defence completed a 'light touch' 'sampling' assessment for five of the six prime external vetting providers, to validate some of the information provided in the DISP membership application.²⁷ Specifically, Defence sought evidence that: the five prime external vetting providers had seven key security governance arrangements in place; and the organisations' security officer had 'an understanding of their DISP security obligations'.²⁸ Defence concluded that:

- two of the five external vetting providers had all seven documents in place;
- two of the five external vetting providers had six of the seven documents in place;
- the remaining external vetting provider had three of the seven documents in place.

2.20 Defence further concluded that four of the five security officers interviewed showed an understanding of their DISP security obligations. The security officer that did not show an understanding of their DISP security obligations worked for the same external vetting provider that had three of the seven security governance arrangements in place.

Cybersecurity questionnaires

2.21 In June 2020 Defence received responses to its cyber security questionnaire from its six prime external vetting providers.²⁹ Defence assigned one of four possible cyber security maturity ratings: 'Embedded'; 'Managing'; 'Developing'; and 'Ad hoc'. Defence assigned four of the six prime external vetting providers a maturity rating of 'Embedded' (the highest rating possible) and two received a rating of 'Managing' (the second highest rating possible).

25 DISO is also responsible for delivering a government commitment to audit the cyber security of defence industry contractors, particularly those involved in the Naval Shipbuilding Plan.

26 Defence provided an extract of this spreadsheet to the ANAO with information concerning its external vetting providers and their sub-contractors.

27 Defence did not assess the sixth provider as it was the subject of a 'deep dive' audit around the same time. The deep dive is discussed in paragraphs 2.22 and 2.23.

28 The seven key security governance arrangements were: Security Register; Evidence of an Insider Threat Program; Evidence of ICT Certification and Accreditation; Physical Certification and Accreditation; Security Plan; Security Policy and Procedures, including ICT; and Security Awareness training package.

29 The stated purpose of the cyber security questionnaire is to help Defence assess the cyber security maturity of the company and the level of probability that the company does not meet DISP requirements.

Deep dive audit

2.22 In September 2020, Defence completed its report of a ‘deep dive’ audit of one of its six prime external vetting providers. The objective of the audit was to assess the security maturity of the provider against the standards listed in the *Defence Security Principles Framework Control 16.1*. Defence concluded that the organisation’s four security domains (governance, personnel security, physical security, and information and cybersecurity) were ‘Developing’.³⁰

2.23 Defence made 10 recommendations to improve the organisation’s compliance with its DISP membership requirements. The external vetting provider agreed to six recommendations and partly agreed to four recommendations. Defence advised the ANAO that to close the audit, Defence will either conduct a follow-up review or request confirmation in writing from the external vetting provider that the audit recommendations have been addressed.

Foreign Ownership, Control and Influence

2.24 The purpose of Defence’s review of Foreign Ownership, Control and Influence (FOCI) information provided in the DISP application is to form a view on whether the provider entity has any FOCI affecting the management or operations of the contracted entity, in a manner which could result in unauthorised access to classified information or adversely affect the performance of contracts.

2.25 As at July 2020, Defence had reviewed the completed FOCI Assessment form for each of its six prime external vetting providers. The review by Defence showed Defence assessed that there were no concerns raised about foreign ownership, control and influence over these providers.

Assurance activities for vetting provider sub-contractors

2.26 Table 2.3 shows the status of the sub-contractors listed in Defence’s tracking spreadsheet for DISP membership application requirements and assurance activities.

Table 2.3: Status of sub-contractor DISP application requirements and assurance activities as at 13 August, 30 September and 30 October 2020

Requirement or activity	Status as at 13 August 2020	Status as at 30 September 2020	Status as at 30 October 2020
FOCI rating	42 (36 per cent) did not have a FOCI rating	11 (9 per cent) did not have a FOCI rating	4 (1 per cent) did not have a FOCI rating
Physical security accreditation	39 (33 per cent) awaiting security accreditation	7 (6 per cent) awaiting security accreditation	No change
Completed security officer training	36 (31 per cent) had not completed security officer training	28 (24 per cent) had not completed security officer training	No change
Sampling assessment	97 (83 per cent) had not provided a sampling assessment	73 (61 per cent) had not provided a sampling assessment	44 (39 per cent) had not provided a sampling assessment

³⁰ This was lower than the June 2020 cybersecurity maturity rating of ‘Managing’ (see paragraph 2.21).

Requirement or activity	Status as at 13 August 2020	Status as at 30 September 2020	Status as at 30 October 2020
Cyber security questionnaire	117 (100 per cent) had not provided a completed cyber security questionnaire	101 (86 per cent) had not provided a completed cyber security questionnaire	37 (33 per cent) had not provided a completed cyber security questionnaire
Total number of sub-contractors	117	117	112 (5 sub-contractors withdrew their application during October 2020)

Note: Data as at 13 August 2020 shows the status of sub-contractor DISP application requirements and assurance activities during ANAO fieldwork. Data as at 30 September 2020 shows the status of applications after ANAO fieldwork was completed, and data as at 30 October 2020 was the most recent data available. Defence advised the ANAO that COVID-19 circumstances slowed the delivery of security officer training.

Source: Defence documentation.

Instances of loss or mishandling of sensitive data

2.27 During the course of this audit, Defence investigated one incident of sensitive data mishandling and identified one incident of sensitive data loss in the past year.³¹

2.28 The first incident occurred on 17 December 2019. A package containing two paper-based personnel security files, sent by a sub-contracted vetting officer to one of the six prime external vetting providers using a regular overnight (door to door) delivery service, was not received.³² A Defence investigation report for the incident stated that the consignment note was dislodged during transit and the courier applied its procedures to identify the package, which included opening the package. The package was identified by the courier and sent to the vetting provider on 20 January 2020. The courier advised the investigator that it had 'offered to discuss with AGSVA different levels of secure services to put in place safeguards', and that if the item had not been opened, it would not have been recovered.³³ Following the incident, in January 2020 Defence directed, via an email instruction to external vetting providers, that all packages must be sent in double envelopes and the destination address affixed to both layers of packaging.

31 Defence provided the ANAO with a spreadsheet showing that there were an annual average of approximately 40,000 file allocations and 40,000 returns of paper-based personnel security files between Defence and external security vetting providers for the financial years 2015–16 and 2019–20. The ANAO did not test the completeness or accuracy of this data.

32 Defence has contracted Toll Group to provide courier services for Defence. Defence advised the ANAO that Toll Group was a member of the previous DISP program and has applied for DISP membership under the strengthened membership requirements. The membership application was submitted to Defence on 29 February 2020, and as at September 2020, Defence was processing the application.

33 Toll Group service costs for delivery of Defence information include: General overnight delivery (standard delivery) (\$7.57); Endorsed overnight delivery (the transport of classified paper based information and ICT based hardware or electronic media rated PROTECTED to TOP SECRET in Australia, with delivery provided office to office) (\$48.67); and Safehand overnight delivery (the transport of classified paper based information and ICT based hardware or electronic media rated PROTECTED to TOP SECRET in Australia. Delivery provided person to person) (\$102.74). A per kilogram charge and further fees and surcharges apply in addition to the basic charge. On this occasion Defence had selected the General overnight delivery (standard delivery) option. Defence advised the ANAO in October 2020 that it is 'reviewing the current process using Toll Group's overnight service and the Toll Group service delivery requirements'.

2.29 The second incident occurred on 16 April 2020, when a paper-based personnel security file for an NV1 clearance was lost during transit while being transported by the courier. Defence tracks the movement of personnel security files through an allocations register, consignment advice emailed between Defence and the external vetting provider, and the use of the courier's consignment tracking portal. On 21 May 2020, Defence was informed by the external vetting provider that the file was unable to be located.³⁴ Defence advised the ANAO that the courier's electronic tracking was not functioning at the time of the incident, and the other mechanisms did not alert Defence that the file had not arrived. Defence further advised the ANAO that it initiated, through the courier firm, national depot searches which did not locate the package.

2.30 On 25 June 2020, Defence informed the affected individual of the loss and advised the individual not to engage with anyone purporting to be from AGSVA, except for nominated AGSVA members. The affected individual was also provided details of the Office of the Australian Information Commissioner and IDCARE (which assists to reduce harm from compromise and misuse of identity information). On 23 July 2020, AGSVA reported the incident to Defence's privacy office. On 31 August 2020 Defence's privacy officer determined the incident was a notifiable data breach and Defence reported the incident to the Office of the Australian Information Commissioner.

2.31 Defence contract managers met with the courier firm to discuss potential improvements following the second incident. Defence advised the ANAO that following the meeting, Defence and the courier put in place new communication arrangements to escalate and improve responses where packages are not delivered in agreed times. A brief to Defence's Associate Secretary dated 20 October 2020 advised on the incidents and Defences' response to the incidents, including that Defence:

- had issued a Contract Notice for all security vetting providers to formally advise on the appropriate notification and escalation processes to be followed if a parcel was delayed or misplaced, and to confirm Defence's and the courier's requirements for packaging and sending parcels. Defence would conduct further verification activities with external vetting providers to ensure appropriate procedures were followed;
- would issue a further Contract Notice to the two external security vetting providers involved in the two security incidents, due to delays in notifying Defence of a missing package. If the correct procedures were not followed in the future, sanctions would be considered;
- was reviewing the courier's service delivery requirements; and
- was assessing options on using alternative ways to allocate personnel security files.

2.32 Defence proposed to provide a regular report on personnel security file management to the Associate Secretary, to ensure the Associate Secretary was informed regarding AGSVA performance and incidents, as Chair of the AGSVA Governance Board. The Associate Secretary noted the response to the incidents, and agreed to the proposal for a regular report, on 31 October 2020.

34 Under contractual arrangements, external vetting providers are required to 'promptly report to the Commonwealth any security incidence ... including instances in which it is known or suspected that security classified information ... has been lost'.

Has Defence implemented the ANAO recommendation contained in the non-public report prepared under subsection 37(5) of the Auditor-General Act 1997?

Defence has partly implemented the recommendation contained in the non-public Auditor-General report provided to the Prime Minister and Ministers. In June 2018, the AGSVA Governance Board was advised that the recommendation had been completed. Defence continued to undertake remediation activities but no further reporting on the progress of remediation activities was provided to the Board. A range of remediation measures were agreed following Defence's assessment that the eVetting system's residual risk rating was 'high' in November 2018. In addition, a life of type extension (LOTE) was agreed and this is subject to continual review of the system. As of September 2020, risk mitigation activities set out in the LOTE had not been completed and reporting on the management of risk to senior whole of government committees, as specified in the LOTE, had not been undertaken. There has been system monitoring and reporting activity internal to Defence.

2.33 Auditor-General Report No. 38 2017–18 *Mitigating Insider Threats through Personnel Security* reported on the ANAO's follow up audit on shortcomings identified in the security of clearance records in Defence's ICT systems during the course of a previous audit, reported on in Auditor-General Report No. 45 2014–15 *Central Administration of Security Vetting*.³⁵

2.34 As part of the second audit the ANAO reported that:

2.52 At the time of the ANAO's previous audit, Defence had conducted two reviews of AGSVA's information security. The reviews had identified that Defence was not compliant with all of the requirements of the Australian Government Information Security Manual and found deficiencies in the controls framework surrounding AGSVA's clearance records which could lead to unauthorised access and loss of information.

2.53 The ANAO conducted further work in this area. In accordance with section 37(1)(a) of the *Auditor-General Act 1997* (Cth) (the Act), the Auditor-General determined to omit particular information relating to this matter, including an additional recommendation to Defence, from this public report. The reason for this is that the Auditor-General is of the view that such information would be contrary to the public interest in that it would prejudice the security, defence or international relations of the Commonwealth, as per section 37(2)(a) of the Act.

2.54 In accordance with section 37(5)(b) of the Act, a report including the omitted information and additional recommendation has been prepared and a copy provided to the Prime Minister, the Attorney-General, the Minister for Defence, the Minister for Finance and the Minister for Home Affairs.

³⁵ The second audit found that 'AGSVA's information systems do not meet its business needs, which has resulted in inefficient processes and data quality and integrity issues' (paragraph 11).

Management of the security of vetting information

2.35 The security of vetting information is provided through Defence's: manual handling requirements for physical file transfers during a vetting assessment; hardcopy personnel file storage facilities; and the eVetting system. The eVetting system comprises:

- the Personnel Security Assessment Management System (PSAMS2) — which acts as a vetting case management system;
- ePack 2 — which allows clearance subjects to complete and submit security vetting packs through an online portal; and
- the Security Officer Dashboard — an online portal that allows security officers in entities to look up limited information about clearance subjects.

2.36 Since 2016, Defence has been implementing a program of work to remediate vulnerabilities in the eVetting system to reduce the assessed level of information security risk.

2.37 After the non-public audit report was provided to the Prime Minister and relevant Ministers on 11 May 2018, Defence advised the Defence Minister in May 2018 that in response to the additional recommendation, Defence:

... plans to realise many process improvements through procuring a new ICT system ... which is expected to be fully operational in 2023. Until the system is fully implemented AGSVA has projects in place to strengthen ICT controls.

2.38 Defence advised the Defence Minister in July 2018 that Defence had implemented the audit recommendation. Defence also informed the AGSVA Governance Board in June 2018 that Defence had implemented the recommendation.³⁶

2.39 Defence has not provided further reporting to the AGSVA Governance Board about the progress of activities to remediate vulnerabilities in the eVetting system. Reporting by Defence on the management of risk in the eVetting system would strengthen the Board's oversight of AGSVA and system-level risks, and would be consistent with the Board's terms of reference, which state that it will provide:

... strategic oversight of AGSVA, including its control and accountability systems. The Board will also monitor the progress of service delivery, business reform and major systems development.

36 The AGSVA Governance Board was established by the Australian Government in 2017 to provide strategic oversight of AGSVA and to monitor the progress of service delivery, business reform and major systems development. The Board is chaired by Defence's Associate Secretary, with membership comprising Senior Executive Service (SES) Band 3 representation from the: Attorney-General's Department; Australian Public Service Commission; Australian Security Intelligence Organisation; Department of Finance; Department of Home Affairs; Services Australia; Department of the Prime Minister and Cabinet; Office of National Intelligence; and Australian Signals Directorate.

Recommendation no.1

2.40 That the Department of Defence supports the Australian Government Security Vetting Agency Governance Board fulfil its terms of reference by reporting to the Board on the management of risk in the eVetting system.

Department of Defence response: *Agreed.*

2.41 *Defence agrees to the recommendation.*

2.42 Defence does not have an established governance process for the implementation of a recommendation contained in a non-public Auditor-General report. The recommendation contained in the non-public report was:

- not recorded in Defence's Audit Recommendation Management System because this system cannot store information classified above the protected level. However, the management action plan for the implementation of recommendations contained in the public audit report (Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security*) noted that the non-public recommendation was completed. The management action plan was signed by the First Assistant Secretary Security and Vetting Services Division on 25 June 2018; and
- not reported to the Defence Audit and Risk Committee, as would normally occur for recommendations made to Defence by the ANAO.

2.43 On 9 July 2018, the Assistant Secretary Vetting reported internally to Defence's Audit and Fraud Control Division that the audit recommendation was implemented and could be closed.

System life of type extension agreed November 2018

2.44 On 2 November 2018 Defence assessed the residual risk of the eVetting system as reduced from 'extreme' to 'high'.³⁷ Defence noted that: 'the time and materials required to re-architect the current system [to further mitigate the identified risks] were unjustifiable', given the estimated cost of project ICT2270 which was expected to remediate the same risks in a comparable timeframe. Defence therefore accepted the 'high' residual risk and agreed to a life of type extension (LOTE) for the system in November 2018.

2.45 The ANAO's review of subsequent internal Defence reporting indicates that remediation activities to reduce the eVetting system's risk level remained incomplete as at September 2020. Of the nine key risk areas, two have been completed, five have been partly completed, and two have not been completed.

2.46 The ANAO identified inconsistencies in Defence documentation relating to the remediation activities. In Defence's technical documentation, the remediation activities are described as being fully and successfully implemented. Defence's eVetting sustainment progress reporting provided to the Assistant Secretary Vetting and the Assistant Secretary Enterprise Technology Operations (in

37 According to the Defence risk rating framework, EXTREME risks are 'too high and must be immediately managed'; HIGH risks are 'probably too high and should be promptly managed by mitigation strategies'; and SIGNIFICANT risks 'should be managed by mitigation strategies as resources allow'.

Defence's Chief Information Officer Group) indicates that remediation activities are only partly completed.

2.47 A second program of remediation activity was agreed within the LOTE (November 2018) to further reduce risk from 'high' to 'significant'. Defence's progress reporting indicates this second program of remediation is partly completed.

Reporting and governance of eVetting system risk

2.48 The November 2018 LOTE system certification is valid until the delivery of a replacement system, and was agreed 'subject to the continual review of the existing system'.

2.49 At an operational level, the existing system is monitored through an eVetting sustainment stakeholder group.³⁸ Meeting records from April to July 2019 and LOTE summary reports from April to August 2020 indicate that Defence is tracking the eVetting risks and LOTE remediation activities.³⁹

2.50 The LOTE was also agreed subject to regular risk reporting to the Secretaries' Cyber Strategy Committee and Government Security Committee.⁴⁰ An eVetting Governance Board was also expected to review and report on the system's risk profile on a six-monthly cycle until the planned decommissioning date of mid-2021. Defence could not provide evidence that the reporting agreed in the LOTE had occurred. Defence should either meet the LOTE requirement for regular risk reporting to the committees listed in the LOTE, or amend the requirement.

38 The group meets weekly and includes representatives from Defence's Chief Information Officer Group, AGSVA and IBM.

39 There is evidence the system experiences instability, with unplanned outages reported up to once a day in July 2019. The ANAO observed numerous unplanned outages during the fieldwork phase of this audit (July and August 2020), that represented approximately 81 hours of lost system operability.

40 The Government Security Committee (GSC) is a whole of government committee providing strategic oversight of protective security policy and informing advice to the Secretaries Committee on National Security. The GSC comprises officials at SES Band 3 level and is chaired by a Deputy Secretary of the Attorney-General's Department.

3. Conditional clearances and sharing of information

Areas examined

This chapter examines Defence’s implementation of the three recommendations made in Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security*.

Conclusion

Defence has implemented the three ANAO recommendations relating to improved processes for conditional clearances and information sharing.

3.1 Three recommendations were directed to Defence in Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security*, relating to improved processes for conditional clearances and information sharing. Defence agreed to implement each recommendation.

3.2 Table 3.1 sets out the recommendations, Defence’s assessment of implementation status and the ANAO’s summary assessment of progress with implementation.

Table 3.1: Assessment of Defence’s implementation of ANAO performance audit recommendations

Recommendation	Defence assessment	ANAO assessment
<p>Recommendation 1:</p> <p>The Department of Defence, in consultation with the Attorney-General’s Department, establish operational guidelines for, and make appropriate risk-based use of, clearance maintenance requirements.</p>	<p>In April 2020, Defence assessed that it had implemented this recommendation.</p>	<p>Defence has implemented this recommendation.</p> <p>See paragraphs 3.7 to 3.17 of this audit.</p>
<p>Recommendation 2:</p> <p>The Department of Defence implement the Protective Security Policy Framework requirement to obtain explicit informed consent from clearance subjects to share sensitive personal information with sponsoring entities.</p>	<p>In July 2018, Defence assessed that it had implemented this recommendation.</p>	<p>Defence has implemented this recommendation.</p> <p>See paragraphs 3.18 to 3.23 of this audit.</p>
<p>Recommendation 3:</p> <p>The Attorney-General’s Department and the Department of Defence establish a framework to facilitate the Australian Government Security Vetting Agency providing sponsoring entities with specific information on security concerns and mitigating factors identified through the vetting process.</p>	<p>In April 2020, Defence assessed that it had implemented this recommendation.</p>	<p>Defence has implemented this recommendation.</p> <p>See paragraphs 3.24 to 3.34 of this audit.</p>

Note: Two of the three ANAO recommendations were also made to the Attorney-General’s Department as it is responsible for supporting entities in the implementation of the Protective Security Policy Framework.

Source: ANAO analysis of departmental documentation.

Enterprise governance arrangements for implementation of ANAO performance audit recommendations

3.3 Defence has established processes to govern the implementation of ANAO performance audit recommendations.⁴¹ In summary the processes involve:

- assigning management responsibility for implementing each recommendation to an individual at the Senior Executive Service (SES) level;
- recording each recommendation in the Audit Recommendation Management System (ARMS) to facilitate tracking the progress of implementation;
- providing advice to the Defence Audit and Risk Committee when recommendations are not implemented by the approved estimated completion date; and
- reviewing evidence of implementation and closing the recommendation.

3.4 In addition to Defence's established processes outlined above, for these three recommendations the AGSVA Governance Board provided additional oversight of, and received updates on, implementation progress.⁴²

3.5 Defence generally followed its established processes to plan, monitor and report on its implementation of the three recommendations. Of the 13 procedures involved, Defence did not fully complete four procedures, namely to: approve the management action plan; update progress monthly in the ARMS; submit timely requests for extensions to the Audit and Fraud Control Division; and maintain records of extensions granted.

Consultation with the Attorney-General's Department

3.6 The two ANAO recommendations concerning conditional clearances (recommendation 1) and the framework for information sharing (recommendation 3) required Defence to consult, or undertake joint action with, the Attorney-General's Department. The ANAO viewed evidence of Defence's consultation with the Attorney-General's Department, and undertaking joint action during the implementation of the two ANAO recommendations, through:

- Defence's membership of the Government Security Committee⁴³;
- the Attorney-General's Department's membership of the AGSVA Governance Board;
- the Secretary of the Department of Defence and the Secretary of the Attorney-General's Department jointly presenting to the Secretaries' Board in February 2020 on progress towards establishing the risk-sharing framework (ANAO recommendation 3); and
- Attorney-General's Department staff participation in Defence's operational level workshops and meetings.

41 These processes did not extend to the additional recommendation made in the non-public Auditor-General report, as discussed in Chapter 2 of this audit report.

42 The Board was discussed in footnote 36.

43 The Government Security Committee is chaired by the relevant Deputy Secretary of the Attorney-General's Department and includes Senior Executive Service (SES) Band 3 or equivalent representation (unless otherwise agreed by the Chair) from the central, security and other agencies. The Committee provides strategic oversight of whole-of-government protective security policy, along with other areas of responsibility.

Has Defence implemented ANAO recommendation 1, to establish operational guidelines for, and make appropriate risk-based use of, conditional clearances?

Defence has implemented ANAO recommendation 1, relating to risk-based clearance requirements. In consultation with the Attorney-General's Department, Defence developed operational guidelines to guide the issuing of conditional clearances. The Vetting Risk Model (VRM) guides vetting officers through the risk factor areas requiring consideration under the Australian Government's Protective Security Policy Framework. Defence's closure of the recommendation in April 2020 was premature as contracted vetting officers did not complete the necessary training and therefore were not using the VRM until September 2020. Defence's advice to the AGSVA Governance Board and the Defence Audit and Risk Committee to close the recommendation did not state the expected completion date of training.

3.7 Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security* found that AGSVA's security clearances did not provide sufficient assurance to entities about personnel security risks, as Defence had not established operational guidelines to apply the Australian Government's protective security policy on conditional clearances. Recommendation 1 of that audit was for Defence to establish, and make appropriate risk-based use of, conditional clearances.

3.8 To assess Defence's implementation of the recommendation, the ANAO examined whether it had been implemented in accordance with the management action plan and whether Defence closed the recommendation appropriately.

3.9 The management action plan stated that Defence would develop, trial and implement the operational guidelines by January 2019. Defence subsequently decided to implement the recommendation after establishing the new external vetting provider panel arrangements in August 2019. The date for implementation was therefore amended from January 2019 to July 2020, and later further amended to September 2020, due to COVID-19 restrictions impacting on the ability to deliver training to contracted vetting officers.

Vetting Risk Model and associated user guide

3.10 To implement the recommendation, Defence, in consultation with the Attorney-General's Department, developed a Vetting Risk Model (VRM) and associated guidelines. The VRM is intended to 'ensure structured and uniform reporting of residual risk as mandated in the Protective Security Policy Framework'.⁴⁴ Defence expect the VRM to 'form the basis of the core risk model within the future vetting system' (the ICT2270 Vetting Transformation project, see Appendix 4) and that:

Once operationalised the system's embedded and integrated, structured risk model will replace the current VRM tool, enabling vetting officers (both internal and external to AGSVA) to complete vetting analysis within the system.

44 At the time of the 2017–18 ANAO audit, Defence conducted security clearance assessments using a Vetting Analysis Report (VAR). The VRM is a form created by Defence using Adobe Acrobat software. Defence describes the VRM as: 'a standardised assessment and decision making method for evaluating insider risk. It is based on a structured professional judgement approach, a methodology which provides for the systematic consideration of factors which have been empirically validated as being risk-relevant and predictive of the issue being assessed (e.g. risk of violence)'.

3.11 The VRM guides vetting officers through the seven risk factor areas identified in the Protective Security Policy Framework (PSPF) to inform a 'whole of person risk rating' and security clearance recommendation. The assignment of risk factor area ratings, the 'whole of person risk rating', and the recommendation to grant, deny or revoke a security clearance are not automatically generated, rather these are decisions made by the vetting officer using their professional judgement.⁴⁵ The completed VRM is then provided to a Defence Australian Public Service (APS) authorised decision maker who decides whether to grant a security clearance.⁴⁶

3.12 Granting a security clearance with conditions may be considered when the vetting officer assigns the clearance subject a whole of person risk rating of either 'moderate-high' or 'high' and 'a recommendation to deny/ revoke the clearance is warranted'.⁴⁷ The VRM user guide states that in this situation the vetting officer is required to initiate a 'procedural fairness process'. If, following the procedural fairness process, Defence determines that the residual risk has not reduced to an acceptable level (through a treatment that is accepted by the sponsoring entity and the clearance subject to manage the realised risk), Defence may determine that a conditional clearance is an appropriate way of managing the residual risk, or may deny the clearance.

3.13 Under the PSPF, Defence can only grant conditional clearances (clearances issued subject to maintenance requirements/conditions) where the sponsoring entity and the clearance subject agree to the proposed maintenance requirements.⁴⁸ This agreement is documented in a 'conditional clearance agreement' negotiated between Defence, the sponsoring entity and the clearance subject.

Risk-based use of clearance maintenance requirements

3.14 In accordance with the management action plan, Defence trialled the VRM by mandating its use by all APS vetting officers, for all new vetting cases, from 1 September 2018. Training of contracted external vetting providers in the use of the VRM started in October 2019 and Defence

45 A whole of person risk rating identifies the overall level of residual risk that a clearance subject carries relevant to their suitability to hold a security clearance. There are four possible risk ratings: low, moderate-low, moderate-high, and high. A vetting officer can recommend to the delegate that a security clearance be denied/revoked or granted/continued. When recommending that a security clearance be granted/continued, the vetting officer can choose to recommend that this be: at a lower level than was requested; with a residual risk advice notice; or with conditions attached (that is, a conditional clearance).

46 The First Assistant Secretary Security and Vetting Services, has delegated to the Assistant Secretary Vetting the authority to appoint certain APS officers as authorised decision-makers. The officers are subject to prescribed qualification requirements and authorised to make particular decisions on certain types of security clearance assessments.

47 The VRM user guide states that a whole of person risk rating of:

- 'moderate-high' suggests that there is at least one concern that is not mitigated; and
- 'high' usually suggests that there are multiple concerns that are not mitigated in current and future contexts.

48 The maintenance requirements are aimed at ensuring the residual risk is managed, by the sponsoring entity and the clearance subject, to an acceptable level. This means reducing the whole of person risk rating to at least moderate-low.

advised the ANAO that all external vetting officers (those employed and sub-contracted) had completed training and were using the VRM from 17 September 2020.⁴⁹

3.15 Defence informed the ANAO of the assurance processes over vetting decisions made using the now superseded form — Vetting Analysis Report (VAR) — during the rollout period:

During the rollout of the VRM, recommendations made by an ESVS [external security vetting supplier] company on a VAR to deny/revoke a security clearance were reviewed internally, and the identified risks and mitigations applied using the VRM. If a case was identified as a grant, with residual risk [that is, a recommendation is made to the delegate to grant a security clearance], a VRM was completed in order to progress with risk sharing. Assurance is provided through the role of the Authorised Decision Maker, internal to AGSVA.

3.16 Defence stores the completed VRM in its case management system (PSAMS2) as an attached document, without a field or flag showing which form (VRM or VAR) was used to support the vetting assessment. Therefore, Defence cannot readily report on the number of clearances processed using each form during the rollout period, without manually checking each clearance. Defence expects that once the ICT2270 vetting system is operationalised (estimated to be Q4 2022):

The system's embedded and integrated, structured risk model will replace the current VRM tool, enabling vetting officers (both internal and external) to complete vetting analysis within the system.

3.17 On 24 April 2020, Defence closed the ANAO recommendation in its Audit Recommendation Management System, and advised the Defence Audit and Risk Committee (DARC) at the committee's July 2020 meeting that the recommendation was closed. Defence's closure of this recommendation in April 2020 was premature, as not all contracted vetting officers had completed training and were therefore not yet using the VRM. Defence's advice to the AGSVA Governance Board and the DARC to close the recommendation did not state the completion date for training.

Has Defence implemented ANAO recommendation 2, to obtain explicit informed consent from clearance subjects to share sensitive personal information with sponsoring entities?

Defence has implemented ANAO recommendation 2, relating to obtaining explicit informed consent from clearance subjects for information sharing. A revised Security Clearance Informed Consent form was introduced from July 2018, as planned. A signed form is a requirement for a security clearance application to be processed.

3.18 Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security* reported that AGSVA's consent form did not explicitly obtain informed consent from clearance subjects to share information with entities. Recommendation 2 of that audit was that Defence obtain explicit informed consent from clearance subjects to share sensitive personal information with sponsoring entities.

49 Defence outsources the assessment of most security vetting cases to external (contracted) security vetting providers. Defence records indicate that external security vetting providers processed 85 per cent of security clearances in 2018, 90 per cent in 2019 and 92 per cent in 2020. Defence advised the ANAO that APS staff make decisions on all vetting cases.

3.19 To assess Defence's implementation of the recommendation, the ANAO examined whether Defence had implemented the recommendation in accordance with the management action plan and reviewed the closure pack that informed the decision to close the recommendation.

3.20 The management action plan stated that Defence would seek legal advice from the Australian Government Solicitor (AGS), integrate that advice into an updated informed consent form, then develop a plan to incorporate the revised form into security clearance procedures. The management action plan stated the recommendation would be implemented by July 2018.

Revised informed consent form

3.21 In June 2018, Defence obtained legal advice from AGS on whether the informed consent form provided sufficient consent to allow Defence to collect and/or disclose the sensitive information of clearance subjects, including specific information on security concerns regarding the clearance subject, and mitigating factors identified through the vetting process, to their sponsoring entities/employing agency. AGS suggested changes to the form, which Defence incorporated into a revised informed consent form. The revised form was implemented from 2 July 2018.⁵⁰ Defence's security clearance procedures do not allow processing to commence until the clearance subject has provided informed consent by way of a signed form.

3.22 On 6 July 2018, Defence closed the recommendation in its Audit Recommendation Management System.

3.23 The ANAO noted during this audit that security clearance procedures had been updated to incorporate the revised form, however there were two instances where procedures referenced the superseded informed consent form. In response, Defence developed a plan to review all of its policies, procedures and guidelines, to ensure they reflect the implementation of the revised informed consent form, the VRM and the risk information sharing framework. Defence advised that it intended to complete this review by 9 October 2020.

Has Defence implemented ANAO recommendation 3, to facilitate AGSVA providing sponsoring entities with specific information on security concerns and mitigating factors?

Defence has implemented ANAO recommendation 3, relating to the provision of information to sponsoring entities. A framework to facilitate Defence providing sponsoring entities with specific information on security concerns and mitigating factors identified through the vetting process was established in October 2019. Implementation of the framework is occurring through a phased approach. Full implementation is expected after the Vetting Transformation project (ICT2270) achieves initial operating capability, which is scheduled for Q4 2022 but remains subject to government consideration.

3.24 Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security* reported that AGSVA did not share information about security concerns outside Defence

⁵⁰ Subsequently, Defence updated the form on 14 August 2018 and on 25 June 2019 (the current version).

and therefore had not met the intent of the Australian Government's 2014 policy reform.⁵¹ Recommendation 3 of the audit was that the Attorney-General's Department and Defence establish a framework to facilitate information sharing.

3.25 To assess Defence's implementation of the recommendation, the ANAO examined whether Defence implemented the recommendation in accordance with the management action plan, and reviewed the closure pack that informed the decision to close the recommendation.

3.26 The management action plan stated that Defence would implement the VRM (discussed in paragraph 3.11), develop protocols and procedures for management and use of shared risk information, develop relevant guidance, trial the framework, seek Government Security Committee endorsement, and implement the framework. Implementation was to be completed by January 2019.

Protective Security Policy Framework requirement to share information

3.27 The Attorney-General's Department issued a revised PSPF in October 2018.⁵² The revised PSPF requires vetting agencies to share relevant 'information of security concern' about security clearance holders with sponsoring entities.⁵³ Under the Personnel Security Adjudicative Guidelines, a determination of whether information is of security concern can only be made by the vetting agency assessing that concern.⁵⁴ Defence will only share information where there is an ongoing risk that is not mitigated, and the information is relevant to managing potential security concerns.

Development of the Personnel Security Risk Information Sharing Framework

3.28 In accordance with the management action plan, the Attorney-General's Department and Defence developed the 'Personnel Security Risk Information Sharing Framework' to facilitate Defence providing sponsoring entities with specific information on security concerns and mitigating factors identified through the vetting process.⁵⁵

3.29 The Personnel Security Risk Information Sharing Framework comprises the VRM and its user guide, and other guidance documents, including:

- the Security Clearance Informed Consent form;

51 In 2014, the Attorney-General's Department revised the PSPF to require Defence to update its informed consent form to allow such disclosure to occur. In October 2016, Defence and the Attorney-General's Department gave a commitment to government that AGSVA would start sharing risk information in 2017–18. AGSVA updated its consent form in February 2017, but the revised form did not explicitly obtain informed consent to share information with entities.

52 Attorney-General's Department, *The Protective Security Policy Framework* [Internet], AGD, available from <https://www.protectivesecurity.gov.au/> [accessed 2 September 2020].

53 The PSPF does not define 'information of security concern'. Defence has developed a threshold for what information of security concern it will share with sponsoring entities as part of the risk-sharing framework.

54 The Personnel Security Adjudicative Guidelines are at Annex A of *PSPF Policy 12 Eligibility and suitability of personnel*. The Guidelines support vetting agencies in their assessment of a person's suitability to hold a security clearance. Attorney-General's Department, *PSPF Policy 12 Eligibility and suitability of personnel* [Internet], AGD, available from <https://www.protectivesecurity.gov.au/personnel/eligibility-and-suitability-of-personnel/Pages/default.aspx#annex> [accessed 2 September 2020].

55 The Personnel Security Risk Information Sharing Framework developed by Defence and the Attorney-General's Department applies only to security clearances processed by AGSVA and does not apply to other authorised vetting agencies.

- document templates to facilitate Defence sharing relevant security risk information with the sponsoring entity;
- processes to share relevant personnel security risk information between Defence and the sponsoring entity, including thresholds for what information Defence will share; and
- a package of guidance and resources to assist agency Chief Security Officers and their support staff to manage personnel security risk information shared by Defence.

3.30 If Defence determines that risk information is to be shared, Defence will share information with sponsoring entities through a Risk Advisory Notice, Residual Risk Advice, or Conditional Clearance Agreement (see Table 3.2).

Table 3.2: Defence’s personnel security risk sharing notifications

Advice notice	When the notification is issued	What information is shared with the sponsoring entity	Why the advice notice is issued
Risk Advisory Notice	Issued during the vetting process if Defence initiates a formal review for cause or procedural fairness process following a preliminary recommendation to deny or revoke a clearance.	The risks that warrant further investigation prior to Defence’s decision to grant/deny a clearance.	To inform the sponsoring entity of any significant risks while the vetting process is underway, so that any temporary mitigations or supports can be put in place until Defence completes the vetting process.
Residual Risk Advice	Issued when Defence has completed the vetting process and granted a clearance on the basis that identified risks have been mitigated to an acceptable level. (Mitigating an identified risk to an acceptable level means that Defence has assessed the residual risk as ‘moderate-low’).	The residual risks and mitigating factors. May include generic optional mitigation measures. Defence may provide specific tailored advice where the general guidance is not sufficient or where the sponsoring entity requests additional guidance.	To inform the sponsoring entity of residual risks, to enable the entity to manage those risks.

Advice notice	When the notification is issued	What information is shared with the sponsoring entity	Why the advice notice is issued
Conditional Clearance Agreement	<p>Issued where Defence has completed vetting process, and has identified unmitigated risks that, if managed through additional conditions, will provide sufficient mitigation.</p> <p>(While the risk is not mitigated it is assessed as being able to be managed through additional conditions. Defence therefore has assessed the residual risk as 'moderate-high' or 'high')</p> <p>Defence will only grant the clearance if the clearance subject, the sponsoring entity and Defence agree to the conditions.</p>	The risks, mitigating factors and appropriate conditions to mitigate the risks.	<p>To inform the sponsoring entity of residual risks, and the mandatory conditions that will mitigate those risks to an acceptable level.</p> <p>To document the agreement between Defence, the sponsoring entity and the clearance subject.</p>

Source: ANAO analysis of Defence documentation.

3.31 The Government Security Committee endorsed the risk sharing framework at its 12 October 2019 meeting and agreed to the implementation plan for the framework at its 12 December 2019 meeting.

Implementation of the Personnel Security Risk Information Sharing Framework

3.32 Defence is implementing the Personnel Security Risk Information Sharing Framework in phases, with priority given to Negative Vetting 2 and Positive Vetting security clearances. Table 3.3 summarises the phases and progress of Defence's implementation of the framework.

Table 3.3: Implementation of the Personnel Security Risk Information Sharing Framework

Phase	Timing and description
Pilot and preparation (Nov 2018 to Dec 2019)	<ul style="list-style-type: none"> Pilot activity (Nov 2018 to Apr 2019) <ul style="list-style-type: none"> Involved two agencies: the Department of Home Affairs and the Australian Taxation Office. Considered Baseline, Negative Vetting 2 (NV2), Negative Vetting (NV1), and Positive Vetting (PV) clearances.
Complete	<ul style="list-style-type: none"> Comprised 126 clearances, the majority (72 per cent) being Baseline and NV1 clearances. Analysis of pilot results, scenario testing workshops with additional agencies, and further refinement of the framework (May 2019 to Nov 2019). The Government Security Committee agreed to the implementation plan for the remaining phases (Dec 2019).

Phase	Timing and description
Phase 1 (Jan to Jun 2020) Complete	<ul style="list-style-type: none"> • Involved nine participating agencies: Department of Home Affairs, Australian Taxation Office, Attorney-General's Department, Australian Federal Police, Austrade, Department of the Prime Minister and Cabinet, Department of Finance, Services Australia, and the Australian Public Service Commission. • Considered all Negative Vetting 2 (NV2), Positive Vetting (PV) clearances, and lower clearance levels for agencies with lower numbers of NV2 and PV clearances. (Approximately 550 active — new, upgrade and revalidation — clearances in progress.) • Completed 264 (new, upgrade and revalidation) clearances — 30 PV and 234 NV2. Of these, Defence: <ul style="list-style-type: none"> – Granted all 264 clearances. – Shared eight pieces of risk information with four agencies through six Residual Risk Notices and two Risk Advisory notices (six were NV2 clearance level and two at PV level). – Did not issue any conditional clearances. • 47 clearance applications were cancelled during the vetting process. • Clearances were processed by Defence APS vetting officers and external security vetting providers (contractors). Defence APS staff made all clearance decisions. • Defence completed a draft report of Phase 1 on 14 September 2020.
Phase 2 (Jul to Dec 2020) In progress	<ul style="list-style-type: none"> • Involves 17 government entities and two Defence Groups (Army and the Capability Acquisition and Sustainment Group). • Will consider all clearances at NV2 and PV levels across all 19 participating organisations. • Expected to comprise approximately 2822 clearances. • In mid-August 2020, Defence advised the ANAO that it had completed 314 clearances across the 19 participating organisations since 1 July 2020, with one instance of risk information being shared with the sponsoring organisation.
Future phases	<p>Defence intends to determine subsequent phases through the AGSVA Governance Board and Government Security Committee.</p> <p>In October 2020, Defence informed the ANAO that:</p> <ul style="list-style-type: none"> • discussions with the Attorney-General's Department about possible future phases have not yet commenced; and • the timeframe for implementing the risk sharing framework to Baseline and NV1 clearances is dependent on the Defence Vetting Transformation project (ICT2270).
Full implementation	<p>Full implementation for all clearance levels (PV, NV and Baseline) across the 570 government (federal, state and territory) and industry bodies relies on capability to be made available through the Defence ICT2270 Vetting Transformation project achieving Initial Operating Capability, which Defence anticipates will be in Q4 2022. In August 2020, Defence informed the ANAO that:</p> <ul style="list-style-type: none"> • 'full implementation across all clearance levels for all entities is reliant on the delivery of ICT2270 Vetting Transformation project due to the volume and manual nature of the current process. The ICT2270 Vetting transformation project will enable sponsoring entities to log in to a secure portal to access risk notices where they exist.' <p>Further detail on the project status of ICT2270 is provided at Appendix 4.</p>

Source: Department of Defence documentation and advice to the ANAO.

3.33 While Defence is implementing the framework in phases, the implementation approach has not impeded the sharing of risk information between Defence and entities which were not part of the pilot, phase one or phase two of the framework's roll-out. Defence advised the ANAO that:

There have been instances of risk information ... being shared with [entities not included in the pilot, phase one or phase two]. These have been managed similarly to the risk sharing framework.

3.34 In February 2020, the Secretaries of Defence and the Attorney-General's Department presented a joint paper to the Secretaries' Board, which included an update on the personnel security risk sharing framework developed by the two departments.⁵⁶

3.35 On 24 April 2020, Defence closed the recommendation in its Audit Recommendation Management System. The Defence Audit and Risk Committee was informed that the recommendation was closed at its 9 July 2020 meeting.



Grant Hehir
Auditor-General

Canberra ACT
7 December 2020

⁵⁶ The Secretaries Board is established by section 64 of the *Public Service Act 1999*, and consists of the following members: the Secretary of the Prime Minister's Department as Chair, the Secretary of each other Department and the Australian Public Service Commissioner.

Appendices

Appendix 1 Department of Defence response



Australian Government
Department of Defence

PO Box 7900 CANBERRA BC ACT 2610

EC20-004191

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

Dear Mr Hehir

Australian National Audit Office Section 19 Proposed Report: Delivery of Security Vetting Services Follow-up

Thank you for your correspondence of 22 October 2020, containing the Proposed Report for the ANAO performance audit – *Delivery of Security Vetting Services Follow-up*.

Defence welcomes the acknowledgement that it has implemented four and partially implemented two of the ANAO and JCPAA recommendations examined by the audit.

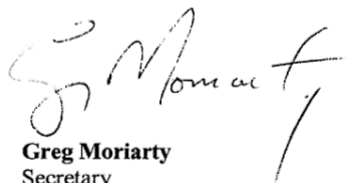
Defence takes seriously the oversight of personnel security vetting and is taking steps to further strengthen the governance of AGSVA and implement your recommendation.

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

Our point of contact is the ANAO Liaison Officer, Nicole Fry, who can be contacted by telephone on 02 6266 3103 or via email at: nicole.fry@defence.gov.au.

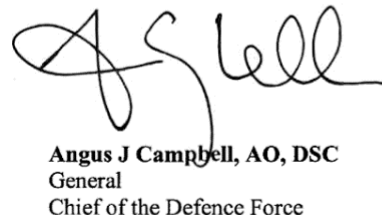
Defence remains committed to assisting you with the successful completion of this audit. We look forward to the upcoming tabling of the Final Report.

Yours sincerely



Greg Moriarty
Secretary

17 November 2020



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

17 November 2020

Appendix 2 AGSVA delivery of vetting services — data

1. As at 1 July 2020, AGSVA maintained 403,888 active security clearances at current clearance levels (Table A.1).⁵⁷ This represents a 36 per cent increase from 295,103 (as at 1 September 2017) reported in Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security*.⁵⁸

Table A.1: Active security clearances, current clearance levels^a, as at 1 July 2020

Clearance level	Classification level of accessible resources	No. of active clearances
Baseline	Up to and including PROTECTED	152,607
Negative Vetting Level 1 (NV1)	Up to and including SECRET	186,734
Negative Vetting Level 2 (NV2)	Up to and including TOP SECRET	48,592
Positive Vetting (PV)	Up to and including TOP SECRET, including certain caveated, compartmented and code word information	15,955
Total		403,888

Note a: AGSVA also manages 107,778 active clearances at security clearance levels issued prior to 2010 which are not included in Table A.1.

Source: ANAO analysis of AGSVA clearance data.

2. Table A.2 shows that over the past three financial years, AGSVA has made an average of 48,504 security vetting decisions annually, with the majority (82 per cent) of decisions at the Baseline and NV1 clearance levels.

57 AGSVA also manages security clearances which were issued prior to 2010 and are not recognised as whole-of-government clearance levels. Previous clearance levels are no longer issued, but 107,778 remain active as at 1 July 2020. Defence has advised the ANAO that these are predominately low level legacy clearances and Defence plans to remediate these clearances when the revalidations fall due, or updated as part of the Vetting Transformation project, whichever comes first.

58 Auditor-General Report No.38 2017–18 *Mitigating Insider Threats through Personnel Security*, p. 17, reported current security clearances as at 1 September 2017.

Table A.2: Security vetting decisions^a by clearance level, 2017–18 to 2019–20^b

Clearance	2017–18	2018–19	2019–20	Average (2017–18 to 2019–20)	All years
Baseline	19,577 (40.75%)	19,377 (40.33%)	20,645 (41.77%)	19,866 (40.96%)	59,599 (40.96%)
Negative Vetting Level 1 (NV1)	21,065 (43.84%)	19,772 (41.16%)	18,938 (38.32%)	19,925 (41.08%)	59,775 (41.08%)
Sub-total Baseline and NV1	40,642 (84.59%)	39,149 (81.49%)	39,583 (80.09%)	39,791 (82.04%)	119,374 (82.04%)
Negative Vetting Level 2 (NV2)	4955 (10.31%)	5209 (10.84%)	6515 (13.18%)	5560 (11.46%)	16,679 (11.46%)
Positive Vetting (PV)	2448 (5.10%)	3683 (7.67%)	3327 (6.73%)	3153 (6.50%)	9458 (6.50%)
Total	48,045 (100.00%)	48,041 (100.00%)	49,425 (100.00%)	48,504 (100.00%)	145,511 (100.00%)

Note a: The ANAO has defined a vetting decision as a decision made by AGSVA between 2017–18 and 2019–20 to grant, deny or revoke a security clearance. This excludes 'reviews for cause', cancellations and other administrative outcomes 'rejected' and 'approved'.

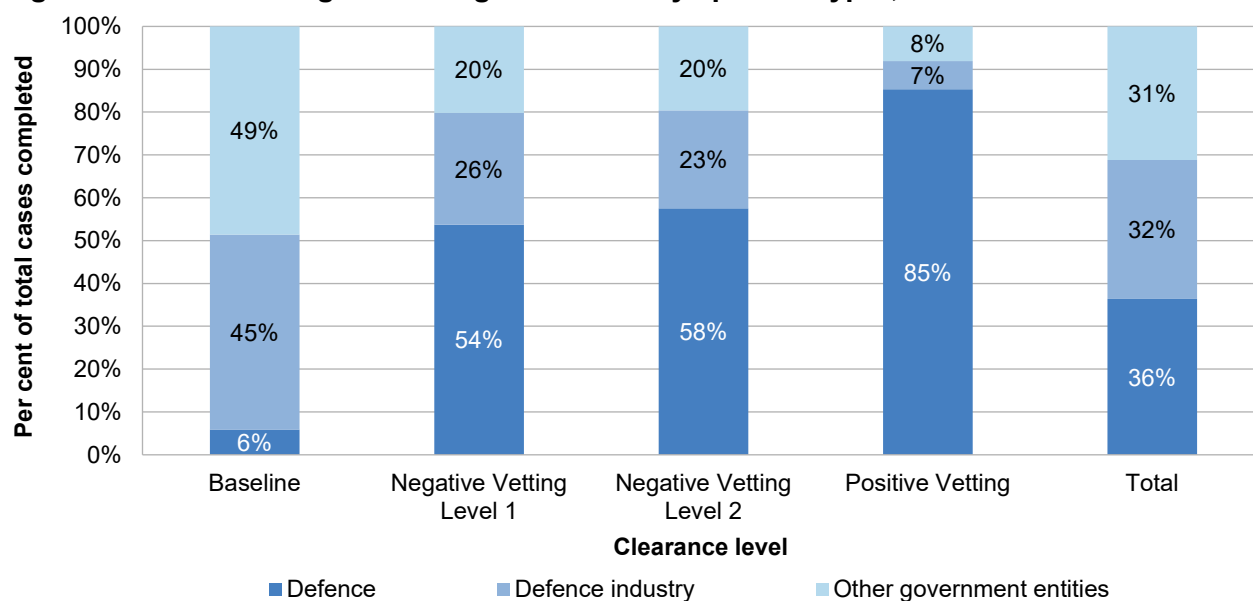
Note b: Data for single years provided by Defence, data for 'average' and 'all years' columns calculated by ANAO.

Source: ANAO analysis of AGSVA clearance data.

3. To request a clearance, the clearance subject must be sponsored by an Australian Government entity.⁵⁹ Defence industry clearances are sponsored by the Department of Defence or by Defence Industry Security Program accredited entities.⁶⁰ For reporting purposes, AGSVA groups clearance sponsors into three categories: Defence, Defence industry and other government entities. Defence and Defence industry combined sponsor the highest proportion of clearances for each clearance level (Figure A.1).

59 Department of Defence, *About Security Clearances – Sponsoring a clearance* [Internet], Defence, available from <https://www1.defence.gov.au/security/clearances/about/sponsoring-a-security-clearance#sponsors> [accessed 21 August 2020].

60 Department of Defence, *Frequently Asked Questions (FAQ)* [Internet], Defence, available from <https://www1.defence.gov.au/security/clearances/about/sponsoring-a-security-clearance> [accessed 29 September 2020].

Figure A.1: Percentage of vetting decisions^a by sponsor type^b, 2019–20^c

Note a: The ANAO has defined a vetting decision as a decision made by AGSVA between 2017–18 and 2019–20 to grant, deny or revoke a security clearance. This excludes 'reviews for cause', cancellations and other administrative outcomes 'rejected' and 'approved'.

Note b: Defence industry includes Defence Industry Security Program (DISP) sponsored and Defence sponsored industry.

Note c: Not all totals add to 100 per cent due to rounding.

Source: ANAO analysis of AGSVA clearance data.

4. For the time period 2017–18 to 2019–20, the outcome of the majority of vetting decisions was to 'grant' a clearance (76 per cent). Table A.3 sets out the outcomes for all clearance cases between 2017–18 and 2019–2020 (Table A.3).

Table A.3: Clearance case outcomes^a by clearance level, 2017–18 to 2019–20

Clearance case outcome	Baseline	NV1	NV2	PV	All levels
Grant	59,591 (76.67%)	59,771 (76.17%)	16,674 (77.38%)	9,425 (69.85%)	145,461 (76.06%)
Deny and grant lower level	0 (0.00%)	2 (0.01%)	2 (0.01%)	29 (0.21%)	33 (0.02%)
Deny	8 (0.01%)	2 (0.01%)	3 (0.01%)	4 (0.03%)	17 (0.01%)
Cancel	15,459 (19.89%)	17,392 (22.16%)	4,692 (21.77%)	3,183 (23.59%)	40,726 (21.30%)
Other ^b	2,665 (3.43%)	1,306 (1.66%)	177 (0.82%)	853 (6.32%)	5,001 (2.62%)
Total	77,723 (100.00%)	78,473 (100.00%)	21,548 (100.00%)	13,494 (100.00%)	191,238 (100.00%)

Note a: Includes initial, upgrade and revalidation cases; excludes 'reviews for cause'.

Note b: 'Other' is comprised of the administrative outcomes 'approved' and 'rejected'.

Source: ANAO analysis of AGSVA clearance data.

Appendix 3 List of recommendations examined

Recommendation	Defence response
<p>ANAO recommendation no.1:</p> <p>The Department of Defence, in consultation with the Attorney-General's Department, establish operational guidelines for, and make appropriate risk-based use of, clearance maintenance requirements.</p>	<p>Defence response: Agreed.</p>
<p>ANAO recommendation no.2:</p> <p>The Department of Defence implement the Protective Security Policy Framework requirement to obtain explicit informed consent from clearance subjects to share sensitive personal information with sponsoring entities.</p>	<p>Defence response: Agreed.</p>
<p>ANAO recommendation no.3:</p> <p>The Attorney-General's Department and the Department of Defence establish a framework to facilitate the Australian Government Security Vetting Agency providing sponsoring entities with specific information on security concerns and mitigating factors identified through the vetting process.</p>	<p>Defence response: Agreed.</p>
<p>ANAO recommendation no.4:</p> <p>Recommendation contained in the non-public Auditor-General report.</p>	<p>Defence response: Agreed.</p>
<p>JCPAA recommendation no. 3:</p> <p>The Committee recommends that the Department of Defence expedite the ICT2270 Vetting Transformation project and provide to the Committee a progress report and updated timeline on implementation of the replacement ICT system.</p>	<p>Defence response: Agreed with qualification.</p> <p><i>Defence agrees with qualification to Recommendation 3 directed towards it by Report 479. Timings of the implementation of the ICT2270 Vetting Transformation project is subject to Defence project governance review and Government approval.</i></p>
<p>JCPAA recommendation no. 4:</p> <p>The Committee recommends that the Department of Defence establish extra safeguards and quality control measures to ensure that no incidents of sensitive data loss occur prior to operational capability of the new vetting case management system.</p>	<p>Defence response: Agreed.</p> <p><i>Defence agrees with Recommendation 4 of the report. Over the last 12 months Defence has put in place a number of additional measures to strengthen security around vetting information as part of wider Defence reform to enhance Defence Industry Security Program (DISP) requirements. The Australian Government Security Vetting Agency (AGSVA) is prioritising resourcing focused on external service provider Information and Communications Technology (ICT) security assurance.</i></p>

Recommendation	Defence response
<p>JCPAA recommendation no. 5:</p> <p>The Committee recommends that the Department of Defence prepare a full business case to consider the current and alternative service delivery models, taking account of projected future demand for vetting, the costs, benefits and risks of various approaches, and provide the findings of this to the Committee within 12 months.</p>	<p>Defence response: <i>Not Agreed.</i></p> <p><i>Defence does not agree with Recommendation 5 of the report. The service delivery model for security clearances has been reviewed extensively in the last decade and is subject to a range of reform and review activities that are currently underway.</i></p>

Appendix 4 Project status — ICT2270

ICT2270 Vetting Transformation project

1. In 2016, the Australian Government agreed a suite of reforms to improve government agencies' management of the threat posed by malicious insiders. The Government noted at this time that Defence would upgrade the Australian Government Security Vetting Agency's (AGSVA) ICT system to support implementation of a number of these reforms. This new capability was intended to support the ongoing assessment of the suitability of security cleared staff, share risk information on clearance subjects between AGSVA and sponsoring entities, and allow vetting agencies to corroborate information provided by clearance subjects with automated links to Commonwealth data sources.
2. The ICT2270 Vetting Transformation project is a key enabler for achieving the government's agenda. In November 2017 Defence told the Defence Investment Committee that:

ICT2270 underpins key elements of the Government's strategy for Mitigating the Malicious Insider Threat, as well as enabling a more automated and efficient vetting service. Government has an expectation that the Sub-Program will begin implementation of a solution to assist with mitigation of the malicious insider threat by 2020. Delays to ICT2270 will result in delays to the WoG [whole of government] reform agenda for security.
3. Defence's August 2019 response to the Joint Committee of Public Accounts and Audit (JCPAA) recommendation to expedite ICT2270 and provide the Committee with a progress report and updated timeline on implementation of the replacement ICT system, noted that first pass government approval had been achieved in April 2018 and second pass was scheduled for Quarter 1 2020.⁶¹ The first pass advice to government noted that the Project was investigating options to accelerate the schedule.
4. Table A.4 shows the key government and Defence decision points for progressing the ICT2270 project since the Government's decision to support a new vetting capability in 2016.

⁶¹ At First Pass, options under consideration are narrowed, and funding is approved for various activities, primarily cost and risk analysis. Second Pass is when government endorses a specific capability solution and approves the funding required for the acquisition phase.

Table A.4: Key decision points for the ICT2270 project

Date	Original timeline	Revised decision	Proposed Defence timeline as of November 2020
October 2016	Government agreement to a suite of reforms to strengthen security policy and practice to more effectively mitigate the threat by malicious insiders.		
April 2017	Defence Investment Committee approval for development of the ICT2270 project (Gate 0).		
November 2017	Defence Investment Committee approval for the ICT2270 project to progress to First Pass consideration by government (Gate 1).		
April 2018	Government First Pass approval for ICT2270.		
September 2019	Defence sought government approval to delay Second Pass, from November 2019 to March 2020.		
December 2019		Defence Investment Committee does not approve ICT2270 project to progress (Gate 2).	
February 2020		Defence obtains government approval to delay Second Pass consideration from March 2020 to late 2020.	
September 2020			Defence Investment Committee approval (Gate 2) for the ICT2270 project to progress to second pass government consideration.
November 2020	Initial Operating Capability		
Late 2020			Planned Second Pass consideration.

Date	Original timeline	Revised decision	Proposed Defence timeline as of November 2020
May 2022		Initial Operating Capability (expected delay of up to 18 months from November 2020)	
Q4 2022			Initial Operating Capability (estimated date approved by Defence Investment Committee, not yet agreed by government)
April 2023	Final Operating Capability	Final Operating Capability	
Q4 2023			Final Operating Capability (estimated date approved by Defence Investment Committee, not yet agreed by government)

Source: ANAO analysis.

5. Table A.4 shows that since Defence provided a project timeline to the JCPAA in August 2019, government has twice approved a delay for second pass consideration for project ICT2270. Defence documentation indicates that the reasons for delay include project complexity and concerns with cost and schedule, which have prompted Defence to assess alternatives.⁶²

6. Subject to government agreement, at Initial Operating Capability Defence is expected to deliver the core vetting system that will replace the current vetting ICT system, which is operating under a Life of Type Extension (see paragraphs 2.44 to 2.47 of this audit report), and replace existing manual business processes (see paragraphs 2.27 to 2.32). Project documentation presented to the Defence Investment Committee in September 2020 for approval (Gate 2) indicates that IOC is estimated to be realised in 2022, with Final Operating Capability to be delivered in 2023, subject to government agreement. Defence estimated that the acquisition costs of the Vetting Transformation project from April 2018 to April 2020 had increased by approximately \$5 million.⁶³

62 The Defence Investment Committee did not agree that the project proceed to second pass consideration on the basis of affordability at Gate 2 on 18 December 2019. The Committee noted that the proposal was not affordable within the Integrated Investment Program (IIP) provision and relied on the Defence Force Structure Plan approved by government in April 2020 (but not released at that time) and ICT sustainment funding offsets that had not yet been approved. The *Defence Force Structure Plan 2020* identifies \$245.5 million in the IIP for ICT2270.

63 Acquisition and capability development costs for ICT2270 were estimated at \$154 million at first pass in April 2018. The *Defence Force Structure Plan 2020* (published 1 July 2020) included \$159.16 million for Vetting Transformation capital.