

# **Mitigating Insider Threats through Personnel Security**

Across Entities

© Commonwealth of Australia 2018

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-346-1 (Print)

ISBN 978-1-76033-346-1 (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 Branch  
Australian National Audit Office  
19 National Circuit  
BARTON ACT 2600

Or via email:

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





Canberra ACT

11 May 2018

Dear Mr President  
Dear Mr Speaker

The Australian National Audit Office has undertaken an independent performance audit across entities titled *Mitigating Insider Threats through Personnel Security*. The audit was conducted in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament.

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

Yours sincerely

A handwritten signature in black ink, reading 'Grant Hehir', is positioned above the printed name.

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**  
**Fax: (02) 6203 7777**  
**Email: [ag1@anao.gov.au](mailto:ag1@anao.gov.au)**

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

### **Audit team**

Daniel Whyte  
Benjamin Siddans  
Alice Bloomfield  
Deborah Jackson

# Contents

---

Summary and recommendations.....	7
Background .....	7
Conclusion .....	8
Supporting findings .....	8
Recommendations.....	10
Summary of entity responses .....	11
Key learnings for all Australian Government entities .....	13
<b>Audit findings.....</b>	<b>15</b>
1. Background .....	16
The trusted insider threat.....	16
The Protective Security Policy Framework.....	16
The Australian Government Security Vetting Agency (AGSVA) .....	17
Entity responsibilities for personnel security .....	19
Current PSPF reforms .....	20
Previous ANAO report.....	21
Rationale for undertaking the audit .....	22
Audit approach .....	22
2. Effectiveness of AGSVA's security vetting services.....	25
Do AGSVA's security clearances provide sufficient assurance about personnel security risks? .....	25
Does AGSVA share relevant information with client entities? .....	34
Does AGSVA have appropriate systems to support its vetting services?.....	38
Does AGSVA have a clear pathway to achieving its benchmark clearance timeframes? .....	41
Does AGSVA have comprehensive quality assurance programs for its contractors and internal vetting decisions? .....	46
3. Entity compliance with personnel security requirements .....	48
Do entities have appropriate risk-based policies, plans and procedures for personnel security? .....	48
Do entities assess the eligibility and suitability of personnel to access government resources? .....	51
Are entities identifying and appropriately mitigating business impacts resulting from security clearance requirements? .....	59
Do entities manage the ongoing suitability of personnel to access government resources? .....	61
Do entities share relevant information with AGSVA?.....	64
Do entities effectively monitor and report on compliance with personnel security requirements?.....	67
<b>Appendices .....</b>	<b>69</b>
Appendix 1 Entity responses .....	70
Appendix 2 PSPF requirements related to personnel security.....	82
Appendix 3 Minimum personnel security checks and requirements for initial clearances .....	84
Appendix 4 AGSVA's clearance timeframes .....	85
Appendix 5 Assessment criteria for personnel security governance.....	87
Appendix 6 Methodology for matching AGSVA clearance holder data and entity personnel data .....	89



# Summary and recommendations

---

## Background

1. The Protective Security Policy Framework (PSPF) outlines a suite of requirements and recommendations to assist Australian Government entities to protect their people, information and assets. Personnel security, a component of the PSPF, aims to provide a level of assurance as to the eligibility and suitability of individuals accessing government resources, through measures such as conducting employment screening and security vetting, managing the ongoing suitability of personnel and taking appropriate actions when personnel leave. In 2014, the Attorney-General announced reforms to the PSPF to mitigate insider threats by requiring more active management of personnel risks and greater information sharing between entities. At the time of the audit, further PSPF reforms were being considered by the Government.
2. The Australian Government Security Vetting Agency (AGSVA) was established within the Department of Defence (Defence) from October 2010 to centrally administer security vetting on behalf of most government entities (with the exception of five exempt intelligence and law enforcement entities). Centralised vetting was expected to result in: a single security clearance for each employee or contractor, recognised across government entities; a more efficient and cost-effective vetting service; and cost savings of \$5.3 million per year. ANAO Audit Report No.45 of 2014–15 *Central Administration of Security Vetting* concluded that the performance of centralised vetting had been mixed and expectations of improved efficiency and cost-effectiveness had not been realised.

## Rationale for undertaking the audit

3. The ANAO chose to undertake this audit because effective personnel security arrangements underpin the protection of the Australian Government's people, information and assets, and the previous audit had identified deficiencies in AGSVA's performance. In addition, the 2014 personnel security reforms occurred after fieldwork for the previous audit had been completed, so there was an opportunity to review the implementation of these reforms by AGSVA and other government entities.

## Audit objective and criteria

4. The objective of the audit was to assess the effectiveness of the Australian Government's personnel security arrangements for mitigating insider threats. To form a conclusion on the audit objective, the ANAO adopted the following high-level criteria:
  - Does AGSVA provide effective security vetting services?
  - Are selected entities complying with personnel security requirements?
5. The entities assessed for criterion two were the Attorney-General's Department (AGD), Australian Radiation Protection and Nuclear Safety Authority (ARPANSA), Australian Securities

and Investments Commission (ASIC), Department of Home Affairs (Home Affairs) and Digital Transformation Agency (DTA).<sup>1</sup>

## Conclusion

6. The effectiveness of the Australian Government's personnel security arrangements for mitigating insider threats is reduced by: AGSVA not implementing the Government's policy direction to share information with client entities on identified personnel security risks; and all audited entities, including AGSVA, not complying with certain mandatory PSPF controls.

7. AGSVA's security vetting services do not effectively mitigate the Government's exposure to insider threats. AGSVA collects and analyses information regarding personnel security risks, but does not communicate risk information to entities outside the Department of Defence or use clearance maintenance requirements to minimise risk. Since the previous ANAO audit, AGSVA's average timeframe for completing Positive Vetting (PV) clearances has increased significantly. AGSVA has a program in place to remediate its PV timeframes, and it has established a comprehensive internal quality framework. AGSVA plans to realise many process improvements through procuring a new information and communications technology (ICT) system, which is expected to be fully operational in 2023.

8. Selected entities' compliance with PSPF personnel security requirements was mixed. While most entities had policies and procedures in place for personnel security, some entities were only partially compliant with the PSPF requirements to ensure personnel have appropriate clearances. None of the entities had fully implemented the PSPF requirements introduced in 2014 relating to managing ongoing suitability. In addition, entities did not always notify AGSVA when clearance holders leave the entity.

## Supporting findings

### Effectiveness of AGSVA's security vetting services

9. AGSVA's clearances do not provide sufficient assurance to entities about personnel security risks. A significant proportion of vetting assessments in 2015–16 and 2016–17 resulted in potential security concerns being identified, but the majority (99.88 per cent) of vetting decisions were to grant a clearance without additional risk mitigation. On rare occasions AGSVA minimised risk by denying the requested clearance level and granting a lower level, or avoided risk by denying a clearance. In some cases identified concerns, which were accepted by AGSVA on behalf of sponsoring entities, should have been communicated to entities or managed through clearance maintenance requirements.

10. AGSVA does not provide information about identified security concerns to sponsoring entities outside Defence due to a concern that disclosure would breach the *Privacy Act 1988*. The PSPF was revised in 2014 to require AGSVA to update its informed consent form to allow such disclosure to occur. Defence and AGD gave a commitment to Government in October 2016

---

1 During the course of the audit, as a result of a machinery of government change, the Department of Immigration and Border Protection became the Department of Home Affairs, incorporating national security and law enforcement policy and operations. For clarity, all references in this report are to its current name.



that AGSVA would start sharing risk information in 2017–18. AGSVA updated its consent form in February 2017, but its revised form does not explicitly obtain informed consent to share information with entities. Consequently, AGSVA has not met the intent of the Government's 2014 policy reform.

11. AGSVA's information systems do not meet its business needs, which has resulted in inefficient processes and data quality and integrity issues. Defence is in the scoping and approval stages of a project to develop a replacement ICT system, which is expected to be fully operational in 2023. The audit included additional work on information security, which is the subject of a report prepared under section 37(5) of the *Auditor-General Act 1997*.

12. AGSVA has recently commenced an organisational renewal project to address identified inefficiencies in its business processes, although it plans to realise many business process improvements through its new ICT system. Since the previous ANAO audit, timeframes for PV clearances have deteriorated significantly; for other levels, the percentage of cases completed within benchmark timeframes has improved.

13. AGSVA has implemented a comprehensive quality audit program for its contractors through its quality management system. It has also introduced periodic internal peer reviews for vetting decisions. It has not instituted a program of independent quality assurance of vetting delegates' decisions.

### **Entity compliance with personnel security requirements**

14. AGD, ARPANSA, ASIC and Home Affairs had plans, policies and procedures in place for personnel security. In some cases, these documents had not been updated to reflect 2014 revisions to PSPF personnel security requirements. DTA had not finalised any of these documents. There was limited evidence of entities undertaking personnel security risk assessments to inform their plans, policies and procedures.

15. AGD, ASIC, Home Affairs and DTA did not have adequate controls and quality assurance mechanisms for ensuring their personnel have appropriate clearances. For each of these entities, a small number of current personnel were identified who did not hold required clearances. Employment screening processes varied across the selected entities. AGD, ASIC and Home Affairs had higher denial rates than AGSVA and made greater use of aftercare.

16. All entities used the temporary access or eligibility waiver provisions of the PSPF to mitigate business impacts resulting from the timeframes to obtain, and eligibility requirements for, security clearances. AGD and Home Affairs used temporary access provisions appropriately to mitigate delays in onboarding personnel. AGD, ARPANSA, ASIC and DTA had not fully complied with PSPF controls for eligibility waivers.

17. AGD, ARPANSA, ASIC and Home Affairs had accessible policies and procedures for managing ongoing suitability, including change of circumstances and contact reporting, and mandatory security awareness training that covered personnel security requirements. DTA had not established these arrangements, as required under the PSPF. None of the entities had implemented the PSPF requirement to conduct an annual health check for clearance holders and their managers.

18. All entities were partially compliant with the PSPF requirement to inform AGSVA when security cleared personnel leave the entity. AGD, ARPANSA and DTA had not updated their employment screening forms to obtain informed consent from personnel to share sensitive information with AGSVA.

19. All entities had reported their compliance with the PSPF personnel security requirements for 2016–17 to relevant parties. The ANAO’s assessment of compliance differed from each entity’s self-reported compliance level.

## Recommendations

**Recommendation no.1**  
**Paragraph 2.24** 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.

**Attorney-General’s Department’s response:** *Agreed.*

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

**Recommendation no.2**  
**Paragraph 2.37** 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.

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

**Recommendation no.3**  
**Paragraph 2.47** 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.

**Attorney-General’s Department’s response:** *Agreed.*

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

**Recommendation no.4**  
**Paragraph 3.6** The Attorney-General’s Department and the Digital Transformation Agency conduct a personnel security risk assessment that considers whether changes are needed to their protective security practices.

**Attorney-General’s Department’s response:** *Agreed.*

**Digital Transformation Agency’s response:** *Agreed.*

**Recommendation no.5**  
**Paragraph 3.9** The Digital Transformation Agency take immediate action to comply with the Protective Security Policy Framework governance requirements.

**Digital Transformation Agency’s response:** *Agreed.*

**Recommendation  
no.6****Paragraph 3.37**

The Attorney-General's Department, the Australian Securities and Investments Commission, the Department of Home Affairs and the Digital Transformation Agency implement quality assurance mechanisms to reconcile their personnel records with AGSVA's clearance holder records, and commence clearance processes for any personnel who do not hold a required clearance.

**Attorney-General's Department's response:** *Agreed.*

**Australian Securities and Investments Commission's response:** *Agreed.*

**Department of Home Affairs' response:** *Agreed.*

**Digital Transformation Agency's response:** *Agreed.*

**Recommendation  
no.7****Paragraph 3.47**

The Attorney-General's Department, the Australian Radiation Protection and Nuclear Safety Authority, the Australian Securities and Investments Commission and the Digital Transformation Agency review their policies and procedures for eligibility waivers to ensure they are compliant with Protective Security Policy Framework mandatory controls.

**Attorney-General's Department's response:** *Agreed.*

**Australian Radiation Protection and Nuclear Safety Authority's response:** *Agreed.*

**Australian Securities and Investments Commission's response:** *Agreed.*

**Digital Transformation Agency's response:** *Agreed.*

**Recommendation  
no.8****Paragraph 3.55**

The Attorney-General's Department, the Australian Radiation Protection and Nuclear Safety Authority, the Australian Securities and Investments Commission, the Department of Home Affairs and the Digital Transformation Agency implement the Protective Security Policy Framework requirement to undertake an annual health check for clearance holders and their managers.

**Attorney-General's Department's response:** *Agreed.*

**Australian Radiation Protection and Nuclear Safety Authority's response:** *Agreed.*

**Australian Securities and Investments Commission's response:** *Agreed.*

**Department of Home Affairs' response:** *Agreed.*

**Digital Transformation Agency's response:** *Agreed.*

**Summary of entity responses**

20. Summary responses from five entities are provided below. Full responses from all entities are provided at Appendix 1.

## **Attorney-General's Department**

Thank you for the opportunity to comment on the proposed audit report on Mitigating Insider Threats through Personnel Security. I welcome the report and I am grateful for the recommendations made to better manage personnel security risks both across Australian Government, and within the Attorney-General's Department.

The timing of this report is helpful noting given the department is currently reforming the Protective Security Policy Framework (PSPF) for application from 1 July 2018. A revised PSPF will provide a clearer and more accessible framework, specify requirements that are proportional to risks, integrate more coherently with other frameworks, and improve the Commonwealth's approach to managing security risk. This report will continue to inform these reforms.

## **Australian Radiation Protection and Nuclear Safety Authority**

ARPANSA welcomed the ANAO audit on our personnel security program and supporting systems. The audit provided a great opportunity for our agency to measure the effectiveness of one element of our protective security program, that being the personnel security component. Importantly, the audit highlighted that, for the most part, ARPANSA has an effective and robust program ensuring the appropriate level of protection for our people, information and assets. The audit identified areas where further efforts can be directed to ensure the agency is proactive in the way we manage eligibility and ongoing suitability of employees and contractors.

## **Australian Securities and Investments Commission**

ASIC welcomes the ANAO's audit into personnel security arrangements. ASIC understands that personnel security is an important function, delivering a level of assurance about the credentials and integrity of our workforce and identifying our vulnerability to a range of insider threats. Throughout the conduct of the audit, ASIC continued to improve its processes and has since implemented procedures to rectify issues identified by the ANAO. ASIC welcomes the findings in the report and considers they provide useful recommendations for improvement in our current practices and reducing the threat from a malicious insider, through enhancements to our personnel security programs.

ASIC concurs with the three recommendations and has updated its Organisational Suitability Assessment to complement the Vetting assessment conducted by the AGSVA. Reforms to our personnel security management aim to achieve compliance with the Protective Security Policy Framework (PSPF). Our key reforms include better identification of security requirements, record keeping and quality assurance, as well as aftercare programs and annual health checks. ASIC confirms that it will implement the recommendations.

ASIC is enhancing its security policies to ensure that they better comply with the PSPF and address the current security threat environment.

## **Department of Defence**

Defence notes the Audit Report on *Mitigating Insider Threats through Personnel Security* (the Report) and the reform efforts already underway to mitigate the malicious insider threat. The Report draws attention to the various aspects of personnel security reform efforts already in development, led by the Attorney General's Department, in close consultation with Defence. Additionally, Defence notes that the Report highlights the internal reform efforts the Australian Government Security Vetting Agency (AGSVA) have undertaken and the improvement in AGSVA's performance over the last two years. AGSVA is still undertaking a significant reform

program with many of the issues flagged in the Report planned for implementation in the next year.

The Report highlights mechanisms for information sharing that will guide agencies to develop clearance maintenance requirements, which are being actively considered and developed by the Attorney General's Department (AGD), as the Commonwealth protective security policy lead. The AGD have overall responsibility for setting the policy parameters, and AGSVA as the main service delivery agency for security vetting.

AGSVA is implementing a program to strengthen security controls within the existing eVetting System, ahead of the delivery of the new system being implemented. AGSVA is working with cross-government and industry partners to ensure that the eVetting System and the systems with which it interfaces meet contemporary security standards.

## Department of Home Affairs

Thank you for the opportunity to provide comments on the ANAO's audit report on Mitigating Insider Threats through Personnel Security.

The Department of Home Affairs responds on the basis that the redactions noted in the report are not relevant to the Department. The report's recommendations appear to be an accurate reflection regarding areas for improvement in Home Affairs.

## Digital Transformation Agency

The Digital Transformation Agency (DTA) agrees with the ANAO's findings and recommendations and will take immediate steps to ensure that all are implemented by 31 July 2018.

## Key learnings for all Australian Government entities

21. Below is a summary of key learnings identified in this audit report that may be considered by other Australian Government entities.

### Procurement

- When procuring a major ICT system that will contain sensitive information, undertaking a thorough risk assessment prior to putting the system into production provides greater assurance that information will be appropriately protected.

### Governance and risk management

- Separating policy and operational functions can lead to implementation challenges. If these functions need to be separate, effective oversight arrangements should be established to avoid silos emerging.
- Sometimes the risks of not sharing information are greater than the risks of sharing it. Entities should comply with privacy and information security requirements, but should not use these provisions as an excuse not to share pertinent information.

### Policy/program implementation

- Policy owners should provide clear, user-friendly guidance and templates that make it easy to comply with policy requirements.



## **Audit findings**

# 1. Background

---

## The trusted insider threat

1.1 On 2 September 2014, the Attorney-General announced changes to the Australian Government's protective security policy to address the threat posed by trusted insiders, stating:

The trusted insider can access—on an unprecedented scale today—massive amounts of sensitive information through our networked computers and copy and transfer it with ease. That is why the two largest breaches of Western intelligence information have occurred only recently.<sup>2</sup>

1.2 The two breaches referred to in the speech were the large-scale leaks of classified information by Edward Snowden in June 2013 and Bradley (now Chelsea) Manning in July 2013; individuals who had been engaged in positions of trust within the United States Government and held security clearances. The Attorney-General noted that these breaches had undermined international efforts to combat terrorism and organised crime, had a detrimental impact on Australia's diplomatic relations, and potentially led to the loss of lives, highlighting the importance of taking action to mitigate insider threats.

## The Protective Security Policy Framework

1.3 The Australian Government's Protective Security Policy Framework (PSPF) outlines a suite of requirements, controls and recommendations to assist Commonwealth entities to protect their people, information and assets. Personnel security—one of the four components of the PSPF<sup>3</sup>—aims to provide a level of assurance as to the eligibility and suitability of individuals accessing Australian Government resources. Key personnel security measures include:

- *Employment screening*—checks, usually undertaken prior to commencement, to establish an individual's identity and assess their suitability to access government resources;
- *Security vetting*—checks undertaken to assess the suitability of an individual to hold a security clearance allowing access to classified information;
- *Managing ongoing suitability*—ensuring individuals with access to government resources continue to meet suitability standards and comply with security measures such as the Contact Reporting Scheme; and
- *Separation actions*—ensuring individuals' access to resources is withdrawn upon separation and they are aware of their ongoing obligations to protect information.

1.4 The policy changes announced by the Attorney-General in September 2014 were primarily revisions to the PSPF personnel security requirements to promote greater information sharing between entities about personnel security risk, and encourage entities to more actively monitor

---

2 Senator the Hon George Brandis QC, Attorney-General for Australia, 'The Insider Threat', speech delivered at 2014 Security in Government Conference, Canberra, ACT, 2 September 2014, available from: <<https://www.attorneygeneral.gov.au/Speeches/Pages/2014/ThirdQuarter2014/2September2014-2014SecurityinGovernmentConference-TheInsiderThreat.aspx>> [accessed 6 October 2017].

3 The other three components are: governance; physical security; and information security. Further information on the PSPF is available from: <<https://www.protectivesecurity.gov.au>> [accessed 7 October 2017].



and manage the ongoing suitability of their personnel. The rationale for these changes was the recognition that several recent malicious insider incidents could have been prevented through more effective information sharing or more active monitoring of personnel demonstrating behaviours of concern.

## The Australian Government Security Vetting Agency (AGSVA)

1.5 The Australian Government Security Vetting Agency (AGSVA) was established within the Department of Defence (Defence) from 1 October 2010 to centrally administer security clearances for most Australian Government entities.<sup>4</sup> Centralised vetting was expected to result in: a single security clearance for each employee or contractor, recognised across government entities; greater consistency in vetting practice; more efficient vetting processes; and cost savings of \$5.3 million per year.

1.6 AGSVA is a branch within the Defence Security and Vetting Service Division. As at July 2017, AGSVA had a staffing profile of 270 full-time equivalent positions, with most staff based in Canberra, Brisbane and Adelaide, and a smaller number of vetting staff based in regional offices across Australia. AGSVA also relies on an external workforce of more than 350 contractors through its Industry Vetting Panel and other contracting arrangements. In 2016–17 AGSVA had an operating budget of \$50 million.

1.7 As at September 2017, AGSVA had 443,172 active security clearances recorded in its Personnel Security Assessment Management System (PSAMS2) database, of which 295,103 were at current clearance levels (see Table 1.1) and 148,069 were at previous clearance levels that were in use until 2010 (see Table 1.2).

**Table 1.1: Active security clearances, current clearance levels, as at September 2017**

Clearance level	Classification level of accessible resources	No. of active clearances
Baseline	Up to and including PROTECTED	114,101
Negative Vetting Level 1 (NV1)	Up to and including SECRET	132,037
Negative Vetting Level 2 (NV2)	Up to and including TOP SECRET	39,258
Positive Vetting (PV)	Up to and including TOP SECRET, including certain caveated, compartmented and codeword information	9,707
<b>Total</b>		<b>295,103</b>

Source: AGD, *Australian Government Personnel Security Protocol*, version 2.1, Canberra, April 2015, pp. 16–17, and ANAO analysis of AGSVA clearance data.

4 Five entities are authorised to undertake their own security vetting: the Australian Federal Police, Australian Secret Intelligence Service, Australian Security Intelligence Organisation, Department of Foreign Affairs and Trade and Office of National Assessments. Other entities must use AGSVA for their security vetting. Prior to 1 October 2010, entities were responsible for conducting their own security clearances. The majority of state and territory government entities also use AGSVA for clearances, although some continue to conduct their own clearances under an agreement with the Australian Government.

**Table 1.2: Active security clearances, previous clearance levels, as at September 2017**

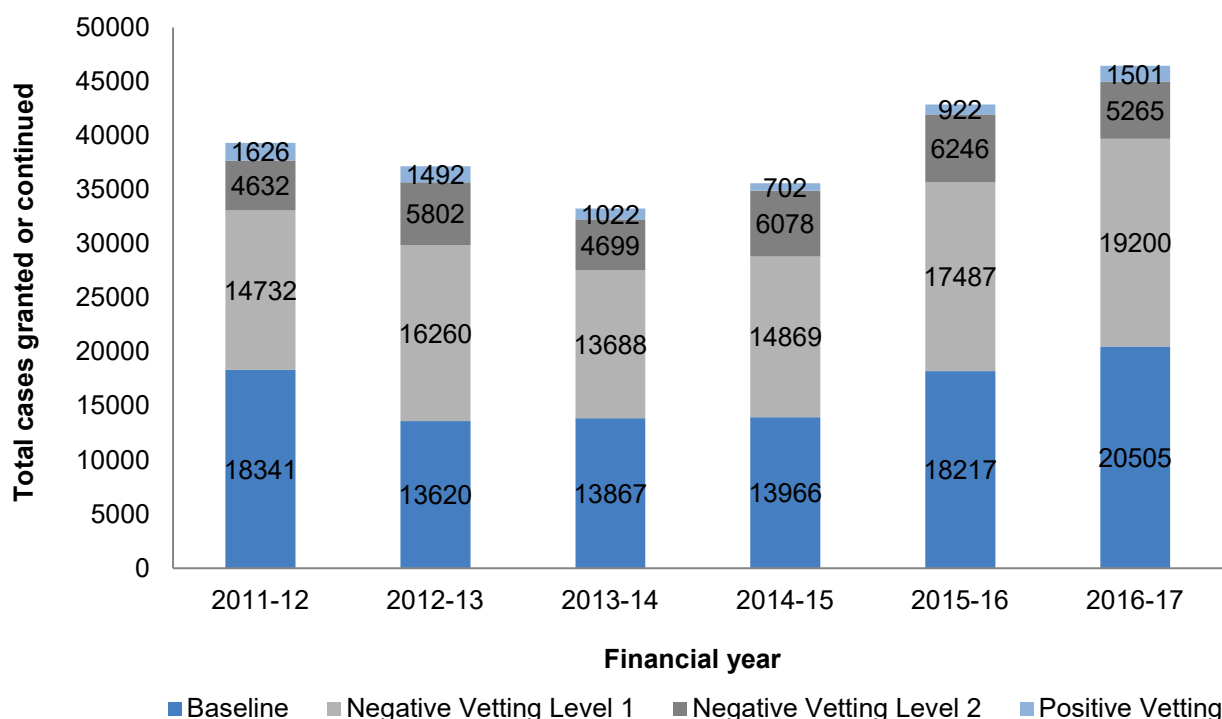
Previous clearance level	Current equivalent clearance level	No. of active clearances
Restricted and Entry <sup>a</sup>	No equivalent (lower than Baseline)	41,168
Protected	Baseline	28,102
Highly Protected	No equivalent (between Baseline and NV1)	7,570
Confidential	No equivalent (between Baseline and NV1)	38,154
Secret	NV1	28,176
Top Secret Negative Vetting	NV2	2,050
Top Secret Positive Vetting	PV	2,849
<b>Total</b>		<b>148,069</b>

Note a: Restricted and Entry level clearances were entity specific levels and not recognised as whole-of-government clearance levels.

Source: ANAO analysis of AGSVA clearance data.

1.8 AGSVA processes a large number of clearance applications each year. Over the past six financial years, AGSVA has made an average of 39,000 vetting decisions each year, with a majority (83 per cent) of decisions at the Baseline and NV1 clearance levels (see Figure 1.1).

**Figure 1.1: Security vetting decisions<sup>a</sup> by clearance level, 2011–12 to 2016–17**

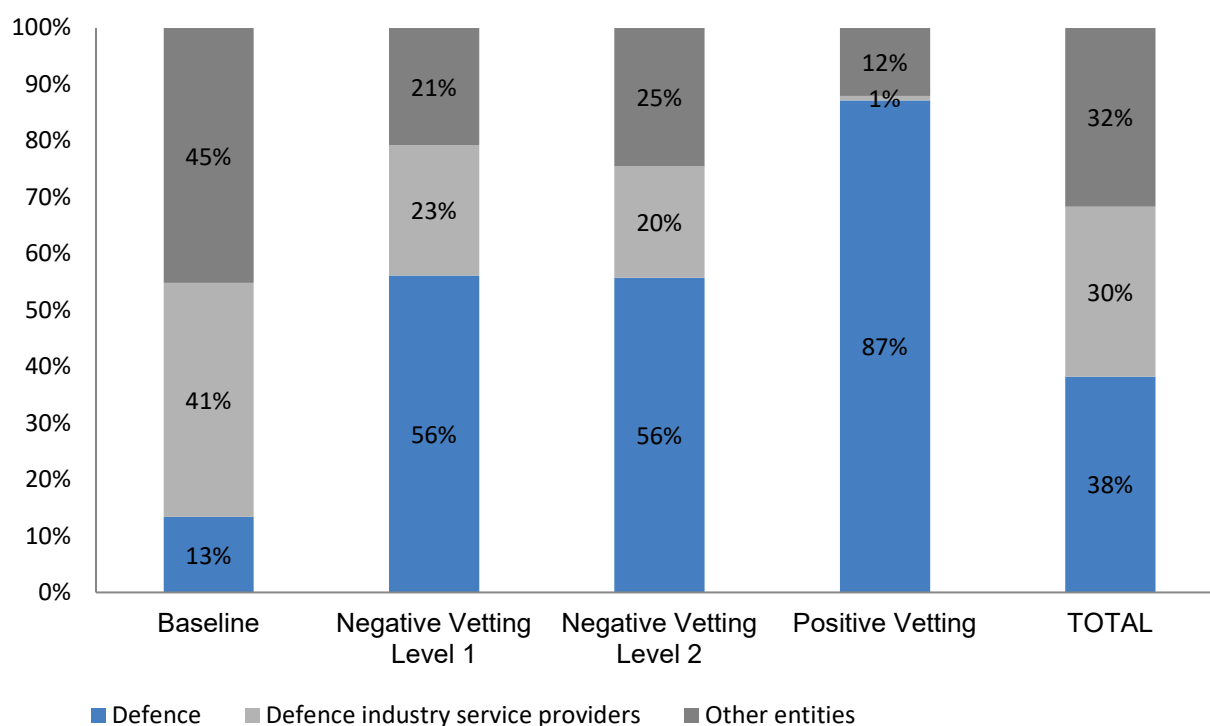


Note a: The ANAO has defined vetting decision as initial and upgrade cases granted or denied and revalidation cases continued or revoked; excludes reviews for cause, cancellations and other administrative outcomes.

Source: ANAO analysis of AGSVA's reported vetting statistics, 2011–12 to 2016–17.

1.9 AGSVA groups clearance sponsors into three categories: Defence; Defence industry service providers; and other entities.<sup>5</sup> The proportion of all security vetting cases finalised in 2016–17 was broadly equivalent across these sponsor types, ranging from 30 per cent for Defence industry service providers to 38 per cent for Defence (see Figure 1.2). However, proportions varied markedly by clearance level: 45 per cent of Baseline clearances finalised in 2016–17 were for other entities; whereas 87 per cent of PV clearances were for Defence.

**Figure 1.2: Percentage of vetting decisions<sup>a</sup> by sponsor type, 2016–17**



Note a: Includes initial and upgrade cases granted or denied and revalidation cases continued or revoked; excludes reviews for cause, cancellations and other administrative outcomes.

Source: ANAO analysis of AGSVA clearance data.

1.10 The services AGSVA delivers, and the responsibilities of clearance holders and the entities that sponsor clearances, are defined in a Service Level Charter. AGSVA is overseen by a Governance Board, comprised of senior representatives from selected sponsoring entities, which considers issues relating to the governance of the Charter. AGSVA also maintains formal agreements with relevant partner agencies, such as the Australian Security Intelligence Organisation (ASIO), which undertakes security assessments for all NV1, NV2 and PV level clearances and Baseline clearances on request.

## Entity responsibilities for personnel security

1.11 Under the PSPF, primary responsibility for protective security rests with portfolio ministers and agency heads. While AGSVA provides security vetting services to government entities, agency

<sup>5</sup> A clearance must be sponsored by an Australian Government entity to be considered active. Defence industry service provider clearances are sponsored by Defence.

heads are ultimately responsible for managing the security risks posed by their personnel. The PSPF's 'Protective security principles' include the principle that:

Agency Heads are to ensure that employees and contractors entrusted with their entity's information and assets, or who enter their entity's premises:

- are eligible to have access
- have had their identity established
- are suitable to have access, and
- are willing to comply with the Government's policies, standards, protocols and guidelines that safeguard that entity's resources (people, information and assets) from harm.<sup>6</sup>

1.12 To meet the intent of this principle, entities must comply with a series of 36 mandatory requirements (the fourteen requirements most relevant to personnel security are outlined at Appendix 2). In addition, entities must adopt mandatory controls, and should adopt better practice recommendations, as outlined in a suite of PSPF personnel security policy documents. At the time of conducting this audit, these documents were:

- 'Australian Government Personnel Security Core Policy' (web page, updated June 2016)<sup>7</sup>;
- *Australian Government Personnel Security Protocol* (April 2015);
- *Personnel security guidelines—Agency personnel security responsibilities* (April 2015);
- *Personnel security guidelines—Vetting practices* (June 2016);
- *Identifying and managing people of security concern—Integrating security, integrity, fraud control and human resources* (January 2015); and
- *Managing the insider threat to your business—A personnel security handbook* (March 2016).

## Current PSPF reforms

1.13 During 2016, AGD led a whole-of-government review of the PSPF in response to the *Independent Review of Whole-of-Government Internal Regulation* (August 2015) (Belcher Review). Recommendations from the Belcher Review relating to security vetting are outlined in Box 1. Recommendation 21.7 reinforced the need for greater information sharing between AGSVA and entities, which (as noted in paragraph 1.4 above) was one of the intended outcomes of the changes to the PSPF announced in September 2014.

1.14 In October 2016, the Government agreed to a suite of measures to strengthen personnel security to mitigate insider threats, to be implemented between 2016–17 and 2018–19, including: developing a framework for assessing ongoing suitability; streamlining and strengthening the vetting process through better use of existing government data holdings; and authorising entities

---

6 AGD, 'Protective security principles', PSPF web page, 29 April 2016, available from: <<https://www.protectivesecurity.gov.au/overarching-guidance/Pages/Protective-security-principles.aspx>> [accessed 7 October 2017].

7 AGD, 'Australian Government Personnel Security Core Policy', 14 June 2016, PSPF web page, available from: <<https://www.protectivesecurity.gov.au/personnelsecurity/Pages/Personnel-security-core-policy.aspx>> [accessed 18 November 2017].

that can meet the required standard to issue Baseline clearances to their own personnel (addressing Recommendation 21.5 of the Belcher Review).

1.15 At the time of conducting this audit, AGD was working with Defence and other relevant entities to implement reforms to the PSPF stemming from its review, with a target date of 1 July 2018 for changes to the PSPF to come into effect.

### Box 1: Belcher Review recommendations relating to security vetting

- 21.5 To reduce the regulatory burden on staff and improve security outcomes, AGD work with Defence and other relevant entities to develop and cost options for reform to personnel security policy which would:
- apply the Principles for Internal Regulation identified in this review, in particular the principle that regulation should be proportional to the risks to be managed;
  - replace Baseline security clearances for ongoing staff with a consistent level of basic employment screening for the Australian Government;
  - reduce the amount of information staff are required to produce for security clearances by electronically seeking information from relevant government and private sources; and
  - develop a continuous evaluation and assessment model for security clearances which, once implemented, would reduce requirements imposed on staff for revalidation of security clearances.
- 21.6 AGD work with the APSC to coordinate work across entities to identify and resolve potential privacy impediments arising from consent requirements for employment screening or security vetting processes.
- 21.7 Defence provide entities with greater visibility of information about security clearance holders identified through centralised security vetting processes to enable those risks to be proactively managed in entities.

Source: Barbara Belcher, *Independent Review of Whole-of-Government Internal Regulation—Report to the Secretaries Committee on Transformation*, volume 1, Canberra, August 2015, p. 40.

## Previous ANAO report

1.16 The ANAO previously reviewed the performance of AGSVA in ANAO Audit Report No.45 of 2014–15 *Central Administration of Security Vetting*, tabled in Parliament in June 2015. The ANAO concluded that the performance of centralised vetting had been mixed and expectations of improved efficiency and cost-effectiveness had not been realised. The ANAO found AGSVA had consistently failed to meet its clearance processing benchmark timeframes, had accumulated a backlog of over 13,000 clearances overdue for revalidation, and had inadequacies with its quality assurance processes, information systems and performance framework. The audit report recommended that Defence:

- implement a targeted audit program to assess Industry Vetting Panel contractors' operations;

- introduce a program of internal peer review supplemented by periodic independent quality assurance of delegate decisions; and
- develop a clear pathway to achieve agreed timeframes for processing and revalidating security clearances.<sup>8</sup>

1.17 In addition, the audit outlined a number of suggestions to improve the effectiveness of AGSVA's operations, including that AGSVA:

- investigate the underlying causes of increasing numbers of clearance subjects cancelling clearances during the vetting process (which peaked at 34 per cent in 2015–16);
- strengthen its controls for managing sensitive personal information captured as part of the vetting process (including details of personnel medical and criminal records);
- improve the quality of its performance measurement and reporting; and
- consider how best to provide feedback to client entities on security concerns identified during vetting, to facilitate those entities' monitoring of affected personnel.

## Rationale for undertaking the audit

1.18 The ANAO chose to undertake this audit because effective personnel security arrangements underpin the protection of the Australian Government's people, information and assets, and the previous audit had identified deficiencies in AGSVA's performance. In addition, the 2014 personnel security reforms occurred after fieldwork for the previous audit had been completed, so there was an opportunity to review the implementation of these reforms by AGSVA and other government entities.

## Audit approach

### Audit objective, criteria and scope

1.19 The objective of the audit was to assess the effectiveness of the Australian Government's personnel security arrangements for mitigating insider threats.

1.20 To form a conclusion on the audit objective, the ANAO adopted the following high-level criteria:

- Does AGSVA provide efficient and effective security vetting services?
- Are selected entities complying with personnel security requirements?

1.21 The audit involved following up on recommendations and suggestions from the ANAO's previous performance audit of AGSVA (ANAO Audit Report No.45 of 2014–15). It also examined selected entities' compliance with PSPF personnel security requirements, with a focus on measures undertaken to mitigate insider threats and communication between AGSVA and client entities on personnel security matters. The assessment of AGSVA focussed on progress since the previous performance audit was tabled in Parliament in June 2015. The assessment of selected entities focussed on compliance during 2015–16 and 2016–17.

---

<sup>8</sup> ANAO Audit Report No.45 2014–15 *Central Administration of Security Vetting*, p. 30.

1.22 Examination of vetting practices within intelligence and law enforcement agencies exempt from using AGSVA's vetting services was out of scope. In addition, the audit did not consider in detail the PSPF reforms being developed by AGD for implementation in 2018. However, where relevant to audit findings, reference has been made within this report to current implementation progress.

### Characteristics of selected entities

1.23 In conducting the audit, the ANAO examined the performance of five selected entities in complying with PSPF personnel security requirements: AGD; Australian Radiation Protection and Nuclear Safety Agency (ARPANSA); Australian Securities and Investments Commission (ASIC); Department of Home Affairs (Home Affairs)<sup>9</sup>; and Digital Transformation Agency (DTA). These entities were selected to provide coverage of a variety of entity functions, locations and sizes.

**Table 1.3: Characteristics of selected entities, as at 30 June 2017**

Characteristic	AGD	ARPANSA	ASIC	Home Affairs	DTA
Function <sup>a</sup>	Policy	Specialist	Regulatory	Larger Operational	Smaller operational
Personnel locations	All states and territories and overseas	NSW and Victoria	All states and territories	All states and territories and overseas	ACT and NSW
Ongoing employees	1,719	128	1,648	13,124	164
Non-ongoing employees	424	19	226	675	34
<b>Total employees</b>	<b>2,143</b>	<b>147</b>	<b>1,874</b>	<b>13,799</b>	<b>198</b>

Note a: Function descriptions as per Australian Public Service Commission classifications.

Source: Australian Public Service Commission (APSC), *Australian Public Service Statistical Bulletin 2016–17*, September 2017, data tables, Excel workbook, available from: <<http://www.apsc.gov.au/about-the-apsc/parliamentary/aps-statistical-bulletin/statisticalbulletin-16-17>> [accessed 17 October 2017].

### Audit methodology

1.24 The major audit tasks included:

- extracting and analysing data from AGSVA's security vetting system, entity human resources information management systems and other relevant databases;
- reviewing entity documentation such as policies, plans, reviews, briefs, procedures, performance reporting, assurance reports, registers and risk assessments; and
- interviewing staff within AGSVA and Defence, in security, human resources and information technology roles within selected entities, and from other relevant entities such as the Australian Security Intelligence Organisation.

9 During the course of the audit, as a result of a machinery of government change, the Department of Immigration and Border Protection became the Department of Home Affairs, incorporating national security and law enforcement policy and operations. For clarity, all references in this report are to its current name.

1.25 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately \$494,000.

1.26 Team members for this audit were Daniel Whyte, Benjamin Siddans, Alice Bloomfield and Deborah Jackson.



## 2. Effectiveness of AGSVA's security vetting services

### Areas examined

The ANAO examined whether the Australian Government Security Vetting Agency's (AGSVA's) security vetting services are effective.

### Conclusion

AGSVA's security vetting services do not effectively mitigate the Government's exposure to insider threats. AGSVA collects and analyses information regarding personnel security risks, but does not communicate risk information to entities outside the Department of Defence or use clearance maintenance requirements to minimise risk. Since the previous ANAO audit, AGSVA's average timeframe for completing Positive Vetting (PV) clearances has increased significantly. AGSVA has a program in place to remediate its PV timeframes, and it has established a comprehensive internal quality framework. AGSVA plans to realise many process improvements through procuring a new information and communications technology (ICT) system, which is expected to be fully operational in 2023.

### Areas for improvement

The ANAO made four recommendations aimed at making greater risk-based use of clearance maintenance requirements, finishing updates to clearance holder consent requirements, providing risk information to sponsoring entities, and remediating ICT control weaknesses.

### Do AGSVA's security clearances provide sufficient assurance about personnel security risks?

AGSVA's clearances do not provide sufficient assurance to entities about personnel security risks. A significant proportion of vetting assessments in 2015–16 and 2016–17 resulted in potential security concerns being identified, but the majority (99.88 per cent) of vetting decisions were to grant a clearance without additional risk mitigation. On rare occasions AGSVA minimised risk by denying the requested clearance level and granting a lower level, or avoided risk by denying a clearance. In some cases identified concerns, which were accepted by AGSVA on behalf of sponsoring entities, should have been communicated to entities or managed through clearance maintenance requirements.

2.1 The purpose of a security clearance is to provide a level of assurance to entities that an individual (the clearance holder) is suitable to access security classified information.<sup>10</sup> Standards for security vetting are specified by the Attorney-General's Department (AGD) in the Protective Security Policy Framework (PSPF) policy document: *Personnel security guidelines—vetting practices* (the vetting guidelines).<sup>11</sup> The vetting guidelines specify the minimum personnel security checks required for Baseline, NV1, NV2 and PV clearances, and outline adjudicative guidelines for

10 AGD, *Australian Government Personnel Security Protocol*, version 2.1, Canberra, April 2015, p. 15.

11 In addition to the PSPF vetting guidelines, the separate *Sensitive Material Security Management Protocol — Personnel — Positive Vetting Guidelines* outline minimum controls for security vetting at the PV level.

vetting officers and delegates for assessing common risk factor areas that may impact on an individual’s suitability to hold a clearance (see Table 2.1 for an overview of factor areas, potential security concerns and mitigating factors).

**Table 2.1: Risk factor areas for assessing suitability to hold a security clearance**

Factor area	Example security concerns	Example mitigating factors
External loyalties, influences and associations	Foreign citizenship, contact with foreign nationals, or substantial financial interests or employment in foreign countries. Involvement in, or association with persons or groups involved in, espionage, terrorism or politically motivated violence.	Reasons for multiple citizenships are not a security concern. Clearance subject was unaware of unlawful aims of an individual or organisation and severed ties upon learning of these.
Personal relationships and conduct	Untrustworthy, unreliable or dishonest conduct. Conduct or contacts that create vulnerability to exploitation, such as high risk or criminal sexual behaviour.	Conduct occurred prior to or during adolescence and there is no evidence of subsequent similar conduct.
Financial considerations	Inability to live within one's means, satisfy debts or meet financial obligations.	Initiated good-faith efforts to repay overdue creditors and otherwise resolve debts.
Alcohol and drug usage	Excessive alcohol consumption, use of illegal drugs or misuse of prescription drugs.	Making satisfactory progress in treatment program and no history of relapse.
Criminal history and conduct	A criminal offence, multiple lesser offences, or association with criminals.	So much time has elapsed that it is unlikely to recur.
Security attitudes and violations	Deliberate or negligent non-compliance with security requirements, such as unauthorised use of ICT systems.	Security violations were due to improper or inadequate training.
Mental health disorders	Certain emotional, mental and personality conditions that may impair judgement, reliability or trustworthiness, or failure to follow treatment advice related to a condition.	Condition is readily controllable with treatment, and clearance subject has demonstrated ongoing and consistent compliance with treatment plan.

Source: AGD, *Personnel security guidelines—vetting practices*, version 1.3, June 2016, section 5.2.

2.2 The vetting guidelines do not specify graduated risk tolerance thresholds for different clearance levels; rather, they outline potentially disqualifying security concerns and mitigating factors that apply to all levels. Higher clearance levels represent increasing levels of assurance that clearance subjects are suitable, based on longer assessment periods (from five years for Baseline to 10 years or from 16 years of age, whichever is greater, for PV) and more rigorous and intrusive testing (see Appendix 3 for the checks required for each clearance level).

2.3 Since AGSVA conducts security vetting services for more than 150 Australian Government entities (as well as state and territory entities), it is not required to provide clearances tailored to specific entity risks. For example, a law enforcement entity may have a lower tolerance for criminal associations or drug usage than other entities, but AGSVA does not consider this distinction when deciding whether to grant or deny a clearance. A clearance granted by AGSVA, which is transferable between entities, provides generic assurance that a clearance holder is

suitable to access classified material, with entities expected to undertake employment screening to address entity-specific risks (discussed in Chapter 3).

## AGSVA's vetting decisions

2.4 A security vetting assessment (or clearance case) can result in several possible outcomes:

- *grant*—grant of a new clearance, or continuation or upgrade of an existing clearance;
- *deny and grant lower level*—denial of the requested clearance level and grant or continuation of a lower clearance level;
- *deny*—denial of a new clearance, or revocation of an existing clearance;
- *cancel*—cancellation of a clearance request (for example, if the clearance subject ceases employment); or
- *other*—other administrative outcomes such as rejecting an incomplete clearance case or downgrading a clearance level due to a change in an entity's requirements.

2.5 The ANAO examined the outcomes of clearance cases completed in 2015–16 and 2016–17 (see Table 2.2). Excluding administrative outcomes (cancel and other), 99.88 per cent of vetting decisions were to grant, 0.06 per cent were to deny and grant a lower level, and 0.06 per cent were to deny a clearance.<sup>12</sup>

**Table 2.2: Clearance case outcomes by clearance level, 2015–16 to 2016–17<sup>a</sup>**

Clearance case outcome	Baseline	NV1	NV2	PV	All levels
<b>Grant</b>	38,713 (70.35%)	36,658 (69.04%)	11,493 (63.68%)	2,407 (31.30%)	89,271 (66.69%)
<b>Deny and grant lower level</b>	4 (0.01%)	14 (0.03%)	16 (0.09%)	21 (0.27%)	55 (0.04%)
<b>Deny</b>	9 (0.02%)	26 (0.05%)	12 (0.07%)	6 (0.08%)	53 (0.04%)
<b>Cancel</b>	13,423 (24.39%)	14,410 (27.14%)	6,064 (33.60%)	4,371 (56.85%)	38,268 (28.59%)
<b>Other</b>	2,877 (5.23%)	1,986 (3.74%)	463 (2.57%)	884 (11.50%)	6,210 (4.64%)

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

Source: ANAO analysis of AGSVA clearance data.

2.6 In addition to clearance cases, AGSVA conducts a small number of reviews for cause, which involve reassessing the suitability of an existing clearance holder due to an identified security concern.<sup>13</sup> AGSVA completed 46 reviews for cause during 2015–16 and 2016–17,

12 The ANAO has defined vetting decisions as: grant; deny and grant lower level; and deny. Cancel and other are considered administrative outcomes, as they do not involve a decision about clearance subject suitability.

13 A review for cause may result from reported changes in a clearance holder's circumstances (discussed in Chapter 3), concerns raised by a sponsoring entity, a security incident involving the clearance holder, or other information received by AGSVA.

resulting in an additional 22 grant, eight deny and grant lower level, and 16 deny decisions (not included in the results in Table 2.2).

### *Management of identified security concerns*

2.7 Personnel security risk is a spectrum in which many clearance subjects demonstrate some behaviours or qualities of concern, and judgement is required to determine if the risk is acceptable. The vetting guidelines provide high level statements about potential security concerns and mitigating factors, so vetting decisions are heavily reliant on the professional judgement of vetting officers and delegates.<sup>14</sup>

2.8 Vetting officers frequently identify potential security concerns during their assessment of a clearance subject, with approximately 43 per cent of all vetting assessments undertaken during 2015–16 and 2016–17 identifying concerns against one or more of the seven factor areas (see Table 2.1 above for descriptions of these factor areas). For clearances granted over this period, the extent to which concerns were identified varied by clearance level (as shown in Table 2.3 below). Since higher clearance levels involve more rigorous checks and cover a longer period of a clearance subject’s life, the rigour of the process may contribute to the identification of more security risk factors (both by increasing the chance a concern will be detected and by discouraging clearance subjects from concealing information from the vetting officer).

**Table 2.3: Identified clearance holder risks for granted clearances, 2015–16 to 2016–17**

Clearance level	Percentage cases with potential concerns identified for factor areas							One or more factors areas
	External loyalties	Relationships & conduct	Financial	Alcohol & drugs	Criminal history	Security attitudes	Mental health	
<b>Baseline</b>	24.46%	0.50%	0.33%	6.83%	4.71%	0.12%	0.72%	32.64%
<b>NV1</b>	30.64%	1.80%	5.61%	12.71%	8.18%	0.53%	3.75%	47.69%
<b>NV2</b>	37.57%	11.71%	11.28%	27.78%	12.94%	2.65%	16.26%	65.95%
<b>PV</b>	44.68%	36.70%	15.37%	45.63%	18.09%	12.47%	43.97%	87.41%

Source: ANAO analysis of AGSVA clearance data.

2.9 To arrive at a vetting decision, AGSVA vetting officers and delegates consider the identified security concerns and mitigating factors and assess the level of residual risk associated with a clearance subject. In broad terms, AGSVA has four options for managing residual risks:

- avoid the risk, by denying the subject a clearance;
- reduce the risk, by modifying controls or implementing further controls, such as granting a clearance with maintenance requirements or granting a lower level clearance;
- share the risk, by granting a clearance and sharing information about identified security concerns and mitigating factors with a sponsoring entity’s security office; or

14 For example, the vetting guidelines state that the amount of time that has elapsed since a transgression can be a mitigating factor, but leave the amount of time to the assessing officer and delegate’s judgement.

- accept the risk, on behalf of a sponsoring entity, by granting a clearance without sharing risk information or implementing clearance maintenance requirements.<sup>15</sup>

2.10 Out of the 89,379 vetting decisions made by AGSVA during 2015–16 and 2016–17 (excluding reviews for cause):

- 53 (0.06 per cent) involved avoiding risk through denying a clearance;
- 55 (0.06 per cent) involved reducing risk through denying the requested level and granting a lower level; and
- two (0.002 per cent) involved reducing risk through granting a clearance with maintenance requirements.

2.11 As discussed later in this chapter (paragraphs 2.30–2.46, pages 34–37), AGSVA does not share risk information with sponsoring entities outside of Defence due to its interpretation of privacy requirements. In the overwhelming majority of cases, AGSVA's approach to managing personnel security risks identified through its vetting process was to accept residual risks on behalf of sponsoring entities.

2.12 AGSVA advised the ANAO that reasons for its relatively low denial rate include:

- rigorous recruitment processes conducted by public sector entities and the Australian Defence Force, which can include pre-employment checks (such as psychological and organisational suitability assessments for Defence intelligence agencies) that exclude personnel on the basis of identified security concerns (discussed in Chapter 3)<sup>16</sup>;
- clearance subjects not complying with the vetting process to avoid security concerns being identified, leading to the cancellation of the clearance; and
- the procedural fairness process, which involves providing an individual who AGSVA is proposing to deny a clearance with an opportunity to respond to identified security concerns, uncovering additional mitigating factors that lead to a grant decision.

2.13 AGSVA's denial rate is also a reflection of its risk appetite—that is, the thresholds it employs for denying a clearance at different clearance levels reflect the levels of residual risk it determines are acceptable. In 2017, AGSVA commenced work to document and standardise its risk tolerance thresholds through the development of a vetting decision risk model, based on work undertaken by AGSVA's psychologists on a structured professional judgement instrument for assessing psychological risk factors. AGSVA informed the ANAO that it plans to start using the risk model in 2018 and subsequently integrate it into its new ICT system, which it anticipates will be fully operational in 2023.

2.14 While development of this model should help AGSVA to codify its risk appetite and aid consistent decision making, there is also scope for AGSVA to make greater use of other risk

15 The Australian Standards AS/NZS ISO 31000:2009 *Risk management—Principles and guidelines* and HB 167: 2006 *Security risk management* identify various options for treating risk: avoiding risk, sharing risk with another party, retaining (or accepting) risk, and modifying controls to reduce the likelihood or consequences of a risk.

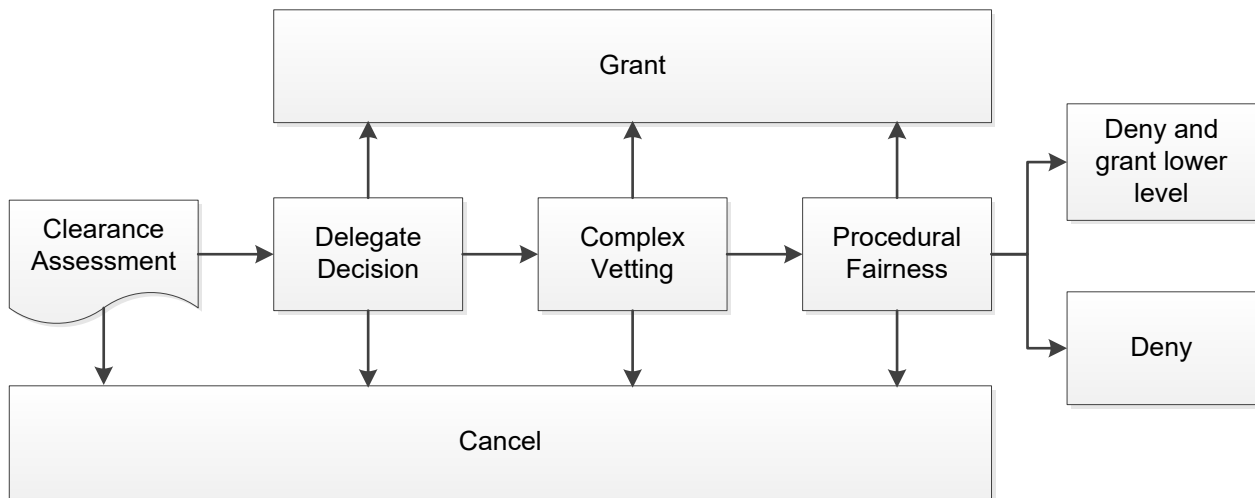
16 ASIO informed the ANAO that the denial rate for its security clearances is significantly higher than AGSVA's. A difference is ASIO conducts security vetting as a component of its employment screening prior to engaging personnel; whereas AGSVA vets personnel who have already been engaged or found suitable by sponsoring entities.

treatment options that involve collaborating with sponsoring entities to manage personnel security risks.

*Resolving doubt in favour of national interest*

2.15 The vetting guidelines state, ‘Any doubt concerning the clearance subject’s suitability must be resolved in favour of the national interest’.<sup>17</sup> However, an internal review of AGSVA, finalised in March 2016, found: ‘The clearance process is over-weighted towards protecting risk to AGSVA through incorrect denial compared with risk to national security’.<sup>18</sup> This finding was based on the observation that, until October 2017, AGSVA’s vetting processes required any case that an initial delegate decided should be a denial to pass through two additional stages of consideration (see Figure 2.1 below).

**Figure 2.1: Denial decision pathway**



Source: ANAO analysis of AGSVA procedural documentation.

2.16 First, a potential denial case progressed to the complex vetting team, where another vetting officer reassessed the case. If the complex vetting officer agreed it should be a denial, it proceeded to procedural fairness, providing the clearance subject with an opportunity to respond to any identified security concerns. After receiving a procedural fairness response, and further consideration by a complex vetting officer and delegate, a final decision to deny or downgrade a clearance was made by the Assistant Secretary Vetting.<sup>19</sup>

2.17 These additional consideration stages greatly increased the time taken to finalise complex vetting decisions (as shown in Table 2.4). Further, at each additional round of consideration a delegate may grant a clearance, increasing the likelihood that an initial deny decision would be overturned. Of the 431 complex cases completed during 2015–16 and 2016–17, 23 per cent were

17 AGD, *Personnel security guidelines: Vetting Practices*, version 1.3, Canberra, June 2016, p. 34.

18 The ANAO notes that AGSVA’s vetting decisions must consider risks to the national interest, which are broader than risks to national security and include impacts on government policies, entities’ operations, personal safety, crime prevention and national infrastructure, and financial and economic impacts.

19 Where a procedural fairness process results in a grant recommendation, the decision may be approved at Assistant Director (Executive Level 1) level; deny decisions require approval by the Assistant Secretary Vetting (Senior Executive Service Band 1).

cancelled prior to a final vetting decision, 53 per cent resulted in a grant, 12 per cent in a denial and grant of a lower level clearance, and 12 per cent in a denial.

**Table 2.4: Case durations for complex and non-complex cases, 2015–16 to 2016–17**

Clearance level	Case type	Number of cases	Average case duration (days)	Benchmark timeframes
<b>Baseline</b>	Non-complex	41,842	27.4	One month (~30 days)
	Complex	37	144.8	
<b>NV1</b>	Non-complex	39,780	123.1	Four months (~120 days)
	Complex	81	640.1	
<b>NV2</b>	Non-complex	12,305	186.9	Six months (~180 days)
	Complex	56	697.2	
<b>PV</b>	Non-complex	3,407	512.6	Six months (~180 days)
	Complex	158	792.6	

Source: ANAO analysis of AGSVA clearance data.

2.18 AGSVA abolished its complex vetting team in October 2017, based on a recommendation of the March 2016 internal review. Going forward, cases subject to a denial decision will proceed directly to the procedural fairness stage.

#### *Use of clearance maintenance requirements*

2.19 The extent to which AGSVA can provide assurance to sponsoring entities regarding personnel security risks is limited by the binary nature of AGSVA's vetting decisions, which generally avoid risk by denying a clearance or accept risk on behalf of a sponsoring entity by granting a clearance.

2.20 The vetting guidelines state that clearances may be granted subject to clearance maintenance requirements (or aftercare), which are specific requirements that a clearance holder must comply with to retain their clearance (such as random drug testing, ongoing treatment for identified mental health issues, or regular reporting).<sup>20</sup> Under the PSPF guidelines, AGSVA is responsible for identifying maintenance requirements and consulting with sponsoring entities and clearance subjects to gain their agreement to any requirements applied. Once implemented, the sponsoring entity and clearance subject are responsible for managing compliance with maintenance requirements and reporting on compliance to AGSVA.<sup>21</sup>

2.21 In 2015–16 and 2016–17, 280 of the 431 complex cases resulted in the grant of a clearance (230 at the requested level, and 50 at a lower level). In all of these cases, the original vetting officer and delegate determined that the clearance should be denied—indicating there was a degree of doubt regarding the level of residual risk. As noted in paragraph 2.10, AGSVA only applied clearance maintenance requirements on two occasions over that period; in both cases for clearances sponsored by Defence. Case study 1 provides an example of a complex vetting case

<sup>20</sup> AGD, *Personnel security guidelines: Vetting Practices*, version 1.3, Canberra, June 2016, p. 55.

<sup>21</sup> AGD, *Australian Government Personnel Security Protocol*, version 2.1, Canberra, April 2015, p. 37.

AGSVA completed for an external entity where clearance maintenance requirements were not imposed but could have been considered. This case study also shows that AGSVA's risk tolerance decisions do not take into account entity employment suitability considerations.

#### Case study 1. Multiple security concerns identified but not communicated to entity

In 2016, a law enforcement entity requested an upgrade of a clearance subject's existing Protected clearance to a NV2 clearance. AGSVA's vetting assessment identified security concerns in five of seven factor areas, three of which were still considered to be a concern after mitigating factors had been identified:

- *alcohol and drug use*—the clearance subject stated they had used illegal drugs several times over the last two decades without the knowledge of their employer, including while holding a clearance and while being assessed for the upgrade, expressed an intention to continue to associate with acquaintances using drugs and did not firmly commit to ceasing drug use;
- mental health issues—the vetting officer had concerns regarding the clearance subject's mental health and ability to recognise their health issues and seek assistance; and
- security attitudes and violations—the clearance subject had failed to properly secure sensitive information on one occasion, and demonstrated other behaviours of security concern.

The vetting officer recommended the clearance upgrade be denied, which was supported by the delegate. Following quality assurance review of the case, the complex vetting team delegate determined that the initial recommendation required reconsideration and an NV2 clearance was granted. The complex vetting officer considered that:

- the clearance subject's drug use and security breaches were sufficiently infrequent;
- the clearance subject appeared to be very honest during the original interview; and
- sufficient 'mitigation' could be found in the case documentation.

Although the clearance subject was employed by a law enforcement entity with a stated 'zero tolerance' policy for personnel using illegal drugs, no information from the case was disclosed to the sponsoring entity, and no clearance maintenance conditions were applied.

2.22 AGSVA informed the ANAO that AGD leads Commonwealth protective security policy and is responsible for setting policy parameters for when and how clearance maintenance requirements should be used and where accountabilities for their implementation lies. As noted in paragraph 2.20 above, PSPF policy documents currently articulate these parameters at a high level. AGD advised the ANAO that, under the proposed 2018 revisions to the PSPF, clearance maintenance conditions will continue to be a shared responsibility of AGSVA, the sponsoring entity and clearance subject.

2.23 Greater use of clearance maintenance requirements would increase the level of assurance provided by AGSVA's security clearances by enabling collaboration between AGSVA and sponsoring entities about managing residual personnel security risks. As part of its current project to develop a vetting decision risk model, AGSVA should establish operational guidelines for appropriate, risk-based use of clearance maintenance conditions. AGD could assist AGSVA in



operationalising this aspect of security vetting policy, by providing input to the development of these guidelines.

### Recommendation no.1

2.24 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.

**Attorney-General's Department's response:** *Agreed.*

*2.25 The department acknowledges the importance of the effective use of clearance maintenance requirements to allow entities to engage with and manage risks associated with their security cleared personnel's access to Australian Government resources. The department commits to providing Defence with information and support to enable AGSVA to make greater use of clearance maintenance requirements. The department will also use existing stakeholder forums to discuss and support the use of clearance maintenance. The department will continue to consult with Defence on the development of a framework to assess the ongoing suitability of security clearance holders, including operational guidelines for sponsoring agencies.*

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

### Cancellation of clearances

2.26 ANAO Audit Report No.45 of 2014–15 suggested that a greater understanding of the reasons for cancellations would assist AGSVA in identifying opportunities for efficiency.<sup>22</sup> Table 2.2 above shows that approximately 28 per cent of clearance cases completed during 2015–16 and 2016–17 ended in cancellation.

2.27 The March 2016 internal review of AGSVA speculated that clearances cancelled during the assessment process may be the result of a deterrent effect, stating:

While no data on the reasons for people cancelling their applications is collected, some of the applicants who cancel out of the process could be doing so because they have found another position while they were waiting for a clearance. For other applicants, the self-cancellation rate could indicate inappropriate applicants dropping out of the system.

2.28 AGSVA's internal analysis of clearance cases cancelled during 2016–17 indicates that 55.6 per cent of cancellations were due to the clearance subject failing to submit a vetting pack or to comply with a request for further information. AGSVA informed the ANAO that some unsuitable individuals may withdraw from the process when they understand the nature of the information being collected.

2.29 As noted in paragraph 2.16 above, around 23 per cent of complex cases were cancelled prior to a final vetting decision, which is lower than the overall cancellation rate. In addition, cancelled complex cases represented only 0.3 per cent of all clearance cancellations. Analysis by the ANAO identified that the majority of cancellations occur prior to AGSVA completing its initial vetting assessment, as shown in Table 2.5. Consequently, there is no clear evidence that clearance

<sup>22</sup> ANAO Audit Report No.45 of 2014–15 *Central Administration of Security Vetting*, p. 65.

subjects cancel their application after becoming aware of a potentially adverse vetting assessment.

**Table 2.5: Stages at which cancellations occur, 2015–16 to 2016–17**

	Baseline	NV1	NV2	PV
Cases cancelled prior to completing factor assessment, with no vetting officer recommendation recorded	13,339 (99.4%)	13,950 (96.8%)	5,921 (97.6%)	4,283 (97.9%)
Cases cancelled after completing factor assessment	82 (0.6%)	464 (3.2%)	146 (2.4%)	90 (2.1%)
<b>Total cancellation cases</b>	<b>13,421</b>	<b>14,414</b>	<b>6,067</b>	<b>4,373</b>

Source: ANAO analysis of AGSVA clearance data.

## Does AGSVA share relevant information with client entities?

AGSVA does not provide information about identified security concerns to sponsoring entities outside Defence due to a concern that disclosure would breach the *Privacy Act 1988*. The PSPF was revised in 2014 to require AGSVA to update its informed consent form to allow such disclosure to occur. Defence and AGD gave a commitment to Government in October 2016 that AGSVA would start sharing risk information in 2017–18. AGSVA updated its consent form in February 2017, but its revised form does not explicitly obtain informed consent to share information with entities. Consequently, AGSVA has not met the intent of the Government’s 2014 policy reform.

2.30 As noted in paragraph 1.4, PSPF policy reforms announced by the Attorney-General in September 2014 were designed to promote greater information sharing and collaboration on personnel risk management between AGSVA and entities. AGD’s revised personnel security policy documents, released in September and November 2014, outlined the following mandatory controls:

Vetting agencies **are to** advise sponsoring agencies of any information provided as part of the vetting process or ongoing clearance maintenance that may impact on a person’s suitability to access Australian Government resources or where risk mitigation measures are required.<sup>23</sup>

Vetting agencies **are to** obtain written informed consent from all clearances subjects to share information with other agencies for the purposes of assessing their ongoing suitability.<sup>24</sup>

2.31 AGD included a sample informed consent form and privacy notice as an annex to the vetting guidelines, which vetting agencies could use to obtain clearances subjects’ written informed consent to share personal information, including sensitive information, with sponsoring

23 AGD, *Australian Government Personnel Security Protocol*, version 2.0, Canberra, 1 September 2014, p. 29. Emphasis in original.

24 AGD, *Personnel security guidelines—Vetting Practices*, version 1.0, Canberra, 4 November 2014, p. 5. Emphasis in original.

entities.<sup>25</sup> AGD obtained advice that appropriate informed consent would allow AGSVA to share such information with entities under the *Privacy Act 1988* (Privacy Act).

2.32 ANAO Audit Report No.45 of 2014–15 noted entities' concerns about AGSVA's level of communication regarding personnel security risks. The audit included a suggestion that AGSVA consider how best to provide feedback to entities on specific security concerns identified during vetting.<sup>26</sup>

2.33 In addition, the Belcher Review recommended that AGSVA provide entities with greater visibility of information on clearance holders to enable them to proactively manage security risks (see Recommendation 21.7 in Box 1 on page 21). The review noted that the Canadian Government's centralised security vetting model allows entities to make the decision on whether or not to grant a clearance based on recommendations from a centralised vetting provider, and information on personnel security risks is provided to entities.<sup>27</sup>

### Revisions to AGSVA's consent form

2.34 AGSVA commenced work on developing a revised informed consent form for its security clearance application pack in late 2014. In February 2017, after a protracted internal debate about the content of the form and subsequent delays in incorporating it into its clearance pack, AGSVA commenced using a revised form, 'SVA 021: Security Clearance Informed Consent and Official Secrecy Acknowledgement'. In informing entity security advisors of the change, AGSVA stated the revisions to the form allowed it to meet the PSPF mandatory control to obtain informed consent from personnel.

2.35 Unlike the sample informed consent form and privacy notice included in the vetting guidelines, AGSVA's form did not explicitly state that it would share sensitive personal information with sponsoring entities for the purpose of assessing their ongoing suitability. Earlier drafts of the form included an explicit statement that AGSVA would share personal information with entities, but the final version of the SVA 021 form did not.

2.36 After publishing its revised form in February 2017, AGSVA came to the view that the form does not provide fully informed consent to share sensitive personal information with entities. As at February 2018, AGSVA had not initiated a project to update the SVA 021 consent form. More than three years after the PSPF was revised to require AGSVA to gain informed consent from clearance subjects, AGSVA has not met the intent of this reform and is non-compliant with the PSPF mandatory control.

---

25 Under the *Privacy Act 1988*, 'personal information' means information or an opinion about an individual, whereas 'sensitive information' includes information or an opinion about an individual's health, political opinions, sexual practices or criminal record—all of which may be collected for security vetting.

26 ANAO Audit Report No.45 2014–15 *Central Administration of Security Vetting*, pp. 106-7 and 109.

27 Barbara Belcher, *Independent Review of Whole-of-Government Internal Regulation—Report to the Secretaries Committee on Transformation*, volume 2, Canberra, August 2015, p. 149.

## Recommendation no.2

2.37 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.

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

### Current information sharing arrangements

2.38 As noted in paragraph 2.5, 99.88 per cent of vetting decisions made by AGSVA resulted in the grant of a clearance. The only information that is routinely shared with entities is that a clearance has been granted at a particular level. Information on potential security concerns and associated mitigating factors identified through the vetting process is not shared with entities.<sup>28</sup>

2.39 In recent years, AGSVA has used a mechanism called 'risk advisory notices' (RANs) to share limited risk information with entities in the following situations:

- *Provisional access requests*—where entities seek to provide individuals with provisional access to classified material prior to clearance being granted, AGSVA can undertake a preliminary review and provide a RAN outlining any generic factor areas in which potential security concerns have been identified (for example, 'Alcohol and drug usage');
- *Direct request*—occasionally entities have requested advice to support an organisational suitability assessment, and AGSVA has made a case-by-case decision on whether to provide a RAN;
- *Change of circumstances*—when a change of circumstances form submitted by an entity or clearance subject has initiated a review of their clearance, AGSVA has occasionally provided a RAN to the sponsoring entity (although in such cases AGSVA noted that the entity is usually already aware of the issue).

2.40 The ANAO examined AGSVA's records of requests to share information from personal security files received during 2015–16 and 2016–17 for any requests received from sponsoring entities.<sup>29</sup> In four instances, each involving Home Affairs, AGSVA released information on the basis of informed consent that the entity had obtained from the clearance subject. In one other instance, involving a different entity, information was not released.

2.41 Over that same period, AGSVA granted 89,271 clearances, 38,925 of which involved identified potential security concerns that were accepted by AGSVA on the basis of mitigating factors. Case study 1 (page 31) provides an example in which AGSVA accepted personnel security risks on behalf of a sponsoring entity without communicating the nature of the risks to the entity.

---

28 With the exception of PV clearances for Defence intelligence agencies, for which there is an established case management process for sharing risk information where there are identified security concerns prior to a vetting decision.

29 The majority of requests to share information from personal security files were requests to transfer files to other vetting agencies or to support an investigation by a law enforcement agency.

2.42 In August 2017, AGSVA advised its whole-of-government oversight forum that:

[RANs] may be seen as pre-empting the assessment process and may result in sanctions that significantly disadvantage the clearance subject and/or expose either AGSVA or the sponsoring agency to appeal or litigation... Additional work and legal advice is required to fully understand the legal and policy constraints of RANs.

2.43 In October 2016, AGD and Defence gave a joint undertaking to Government that AGD would identify solutions to allow AGSVA to share information with entities in 2016–17 and AGSVA would implement information sharing within the vetting process in 2017–18.

2.44 Planning documents for Defence's 'ICT2270 Vetting Transformation' project (discussed in the next section) indicate it intends to integrate the capability to share risk information with external entities within this new system. The new ICT system is not expected to be fully operational until 2023.

2.45 When AGSVA updates its informed consent form, in line with Recommendation no.2 (paragraph 2.37), at the same time it should revise its business processes to enable it to routinely provide sponsoring entities with risk information about clearance subjects, during the vetting process (for provisional access requests), at the point of granting a clearance, and when an entity sponsors an existing clearance. This will allow entities to consider, in light of their individual risk tolerances, whether identified security concerns warrant further treatments (such as requiring individuals to provide regular updates to the security office on matters of concern).<sup>30</sup>

2.46 As AGD is responsible for security vetting policy and Defence is responsible for whole-of-government vetting operations, they should work together to develop operational policies and guidelines that specify:

- what level of risk information should be shared and in what form;
- who within entities it should be shared with (for example, an entity's security advisor or security executive); and
- any caveats or restrictions that should be placed on entities' use of risk information.

---

30 In addition to any clearance maintenance requirements imposed by AGSVA in line with Recommendation no.1.

### Recommendation no.3

2.47 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.

**Attorney-General's Department's response:** *Agreed.*

2.48 *The department acknowledges the importance of communicating risk information to sponsoring entities and other vetting agencies as part of the initial process of security vetting and to support the ongoing assessment of personnel's suitability to hold a security clearance. Sharing security relevant information within an entity and between entities is essential to appropriately safeguard Australian government resources and can help prevent and detect a range of threats, including the trusted insider threat.*

2.49 *The department, in consultation with Defence and a number of other departments and agencies, is developing a range of resources to support risk information sharing such as clearance suitability risk factor guidelines and a fact sheet on information sharing to address misconceptions about perceived limitations to information sharing, as well as specific mechanisms such as templates and guidance to support Defence, and other vetting agencies, in sharing risk information with sponsoring entities.*

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

### Does AGSVA have appropriate systems to support its vetting services?

AGSVA's information systems do not meet its business needs, which has resulted in inefficient processes and data quality and integrity issues. Defence is in the scoping and approval stages of a project to develop a replacement ICT system, which is expected to be fully operational in 2023. The audit included additional work on information security, which is the subject of a report prepared under section 37(5) of the *Auditor-General Act 1997*.

2.50 AGSVA's vetting services are supported by the eVetting system<sup>31</sup>, which from an end-user perspective consists of three primary components:

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

---

31 In addition to its vetting-specific systems, AGSVA also relies on systems used by many areas of Defence, such as records management systems to store electronic documents.

2.51 ANAO Audit Report No.45 of 2014–15 identified shortcomings in AGSVA's ICT systems relating to the security of clearance records, data quality and the ability of the systems to support AGSVA's business processes.

### Security of clearance records

2.52 At the time of the ANAO's previous audit, Defence had conducted two reviews of AGSVA's information security.<sup>32</sup> 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.<sup>33</sup>

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.

### Data quality

2.55 The ANAO's previous audit of AGSVA identified data quality issues with clearance records held in the eVetting system, such as the presence of duplicate records and date-related anomalies.<sup>34</sup> Anomalies of this nature continue to be present within the eVetting system.<sup>35</sup>

2.56 AGSVA is heavily reliant on manual review by staff to detect data quality issues in new clearance requests submitted by sponsoring entities, such as incorrect dates of birth, duplicate records and missing information. AGSVA does not require clearance holders to verify their personal information, and relies on change of circumstances reports from clearance holders and sponsoring entities to ensure its biographical records are up to date (discussed in more detail in Chapter 3).

2.57 The ANAO did not systematically verify the quality of AGSVA's clearance data holdings, but was able to identify obvious errors and discrepancies in the biographical data of clearance holders. Examples of these issues are shown in Table 2.6.

---

32 These reviews were a November 2014 Information Management Review and a February 2015 Threat and Risk Assessment.

33 ANAO Audit Report No.45 2014–15 *Central Administration of Security Vetting*, pp. 87-88.

34 ANAO Audit Report No.45 2014–15 *Central Administration of Security Vetting*, p. 86.

35 Legacy clearance holdings are clearances at previous clearance levels that were in use until 2010, which are discussed in paragraph 1.7.

**Table 2.6: PSAMS2 data quality issues**

Measure	Number of cases, as at 11 September 2017	Number of cases with decisions made between 1 January 2017 and 11 September 2017
Clearance holder aged over 100	5	1
Clearance holder aged under 10	65	1
Clearance holder date of birth in the future	3	0
No recorded location of birth	89,282	3,774
Active primary clearances with revalidation dates more than five years in the past	194	57
Probable duplicate clearance subject records <sup>a</sup>	2,238	N/A

Note a: The ANAO considered a clearance subject record to be a probable duplicate if first name, family name, year of birth, birth location and primary sponsoring entity were identical to at least one another record.

Source: ANAO analysis of AGSVA clearance data.

2.58 AGSVA should take a more proactive approach to identifying, preventing and resolving anomalous data. In late 2017, AGSVA commenced a pilot project with a single sponsoring entity to validate clearance subject data, with an aim of initiating a project in 2018 to further validate clearance holdings in advance of transferring information to its new ICT system.

### Supporting AGSVA's business processes

2.59 AGSVA's current case management system, PSAMS2, supports vetting officers to manage clearances by providing workflow guidance. It automatically generates tasks (such as reviewing a file, undertaking an external check, or making an assessment decision) for completion by AGSVA vetting officers and delegates. However, it does not enforce completion of all tasks, even when such tasks are required to issue a clearance. As at September 2017, the ANAO identified three cases relating to PV clearances from 2015–16 and 2016–17 that had progressed to a vetting decision without an ASIO check being completed. After the ANAO advised AGSVA of this, AGSVA informed the ANAO that it would develop a custom report for its database to identify any cases where this may have occurred.

2.60 Limitations in PSAMS2 also reduce AGSVA's ability to measure its performance. The system records the date at which major milestones have been completed, allowing for broad measurement of timeliness, but identification of bottlenecks and inefficiencies could be improved with more granular information about when subtasks are completed. Similarly, the system only permits one case type (or system task) to be active on a clearance holder's record at one time, which reduces AGSVA's ability to quantify and analyse its work processes. For example, if a clearance upgrade case is in progress and AGSVA receives a change of circumstances report, the change of circumstances case will not be separately recorded.

2.61 A significant portion of AGSVA's vetting services are undertaken by contractors on its Industry Vetting Panel. Due to concerns about system stability, AGSVA has not been able to provide its contractors with access to PSAMS2, which means clearance records are communicated via both mail and email. As a result, contractors accumulate a considerable volume of hard-copy and electronic information, over which AGSVA has limited oversight. In addition, potentially



sensitive information is communicated outside of Defence's secure ICT environment. AGSVA's Industry Vetting Panel deed requires contractors to comply with Defence's information security policies, but AGSVA's internal quality assurance reviews of contractors (discussed later in the chapter) have identified that these requirements were frequently not adhered to.

### *ICT2270 Vetting Transformation project*

2.62 Defence is aware that the eVetting system does not meet AGSVA's needs, and has a commenced an 'ICT2270 Vetting Transformation' project to develop a replacement system. The project is currently in the initial scoping and approval stages. Project documentation indicates Defence seeks to establish a system that:

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

2.63 In September 2017, in a brief to the incoming Secretary of Defence, AGSVA indicated that 'delivery of an initial operating capability' was envisaged in 'late 2020'. A subsequent paper to its Governance Board in December 2017 indicated that, while initial capability was still expected to be delivered in 2020, the system would not be fully operational until 2023.

## **Does AGSVA have a clear pathway to achieving its benchmark clearance timeframes?**

AGSVA has recently commenced an organisational renewal project to address identified inefficiencies in its business processes, although it plans to realise many business process improvements through its new ICT system. Since the previous ANAO audit, timeframes for PV clearances have deteriorated significantly; for other levels, the percentage of cases completed within benchmark timeframes has improved.

2.64 ANAO Audit Report No.45 of 2014–15 highlighted AGSVA's longstanding inability to meet agreed performance targets for processing security clearances and to address its mounting backlog of clearances due for revalidation. The report discussed the need for Defence to 'develop a pathway—including agreed strategies, targeted resources and a timetable—to improve its performance against benchmark timeframes, and address the revalidation backlog at a time of heightened focus on the threat posed by trusted insiders'.<sup>36</sup>

### **Management of AGSVA's vetting caseload**

2.65 AGSVA's processes for managing its vetting caseload are inefficient. As discussed in paragraphs 2.59 to 2.61, AGSVA's business systems do not adequately support its needs, and the functionality and information required to effectively manage its caseload is not always available. Internal reviews of AGSVA have also identified shortcomings in business processes that contribute to inefficient caseload management, including:

<sup>36</sup> ANAO Audit Report No.45 2014–15 *Central Administration of Security Vetting*, pp. 101–2.

- the clearance pack being transferred to and from paper to digital documents three to five times during the vetting process, with corresponding manual copying or data entry of the entire clearance pack into PSAMS2<sup>37</sup>;
- clearance applications being re-checked and re-vetted multiple times, particularly where cases are recommended for denial; and
- applications following the same process regardless of risk and vetting resources not being allocated based on risk.

2.66 In mid-2017, AGSVA initiated an organisational renewal project, which has involved implementing preliminary measures to address these inefficiencies, including:

- developing a new cost model for determining the price of security clearances charged to sponsoring agencies (to be implemented from early 2018);
- abolishing the complex vetting unit and redesigning the vetting process to allow vetting officers to undertake procedural fairness without the need to re-vet cases (implemented from October 2017); and
- undertaking a pilot program, from March to August 2017, to create unified vetting teams, allowing resources to be allocated more efficiently (previously PV clearances were managed by a separate teams to Baseline, NV1 and NV2 clearances).

2.67 While these are positive developments, AGSVA plans to realise other business process improvements through its new ICT system, which is not expected to be fully operational until 2023.

### Revisions to AGSVA’s benchmark clearance timeframes

2.68 AGSVA’s original benchmark clearance timeframes were outlined in its 2010 Charter and remained unchanged in successive Service Level Charters until the end of 2016–17. In June 2017, AGSVA gained agreement from its Governance Board to revised timeframes and key performance indicators for 2017–18, to be reviewed annually going forward. The original and revised benchmark timeframes and performance reviewed targets are in Table 2.7.

**Table 2.7: AGSVA’s benchmark clearance timeframes and targets, original and revised**

Clearance level	2010–11 to 2016–17		2017–18	
	Original benchmark timeframe	Performance target	Revised benchmark timeframe	Performance target
<b>Baseline</b>	One month	95 per cent of cases within benchmark	20 business days	Average processing time for routine cases <sup>a</sup> within benchmark
<b>NV1</b>	Four months		90 business days	
<b>NV2</b>	Six months		125 business days	
<b>PV</b>	Six months		180 business days	
<b>PV Priority</b>			90 business days	

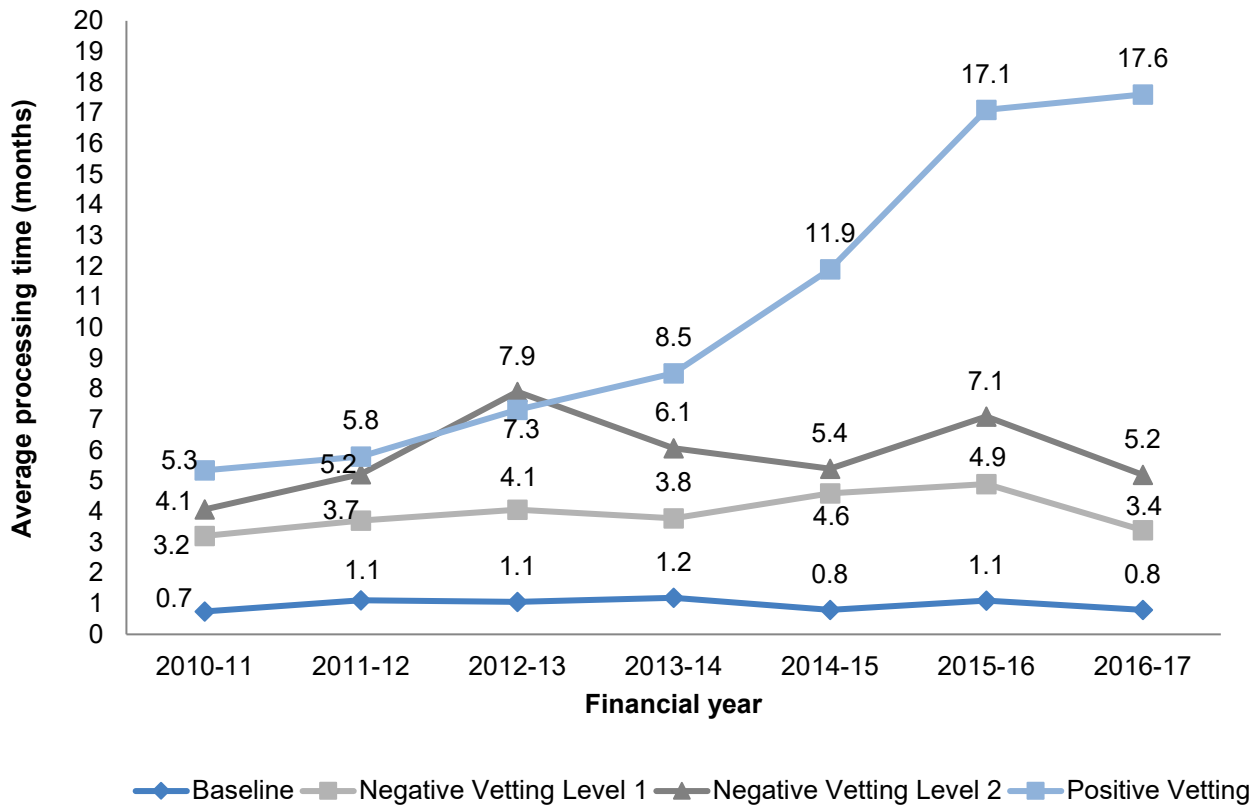
Note a: AGSVA defines ‘routine cases’ as excluding cancellations.

Source: AGSVA Service Level Charters.

37 AGSVA advised the ANAO that its current procedures involve transferring packs from paper to digital twice and, for the approximately 10 per cent of cases completed in-house, cases are completed digitally.

2.69 Since 2010–11, AGSVA's average processing times for Baseline, NV1 and NV2 clearances have fluctuated at around the original benchmark timeframes (see Figure 2.2), with its best performance in 2010–11—its first year of operation. AGSVA's average processing time for PV clearances has increased steadily, reaching a peak of 17.6 months in 2016–17. As at September 2017, AGSVA was on track to achieve its revised 2017–18 performance target for Baseline, NV1 and NV2 clearances, but not PV clearances.

**Figure 2.2: Average processing time for clearance cases by level, 2010–11 to 2016–17**



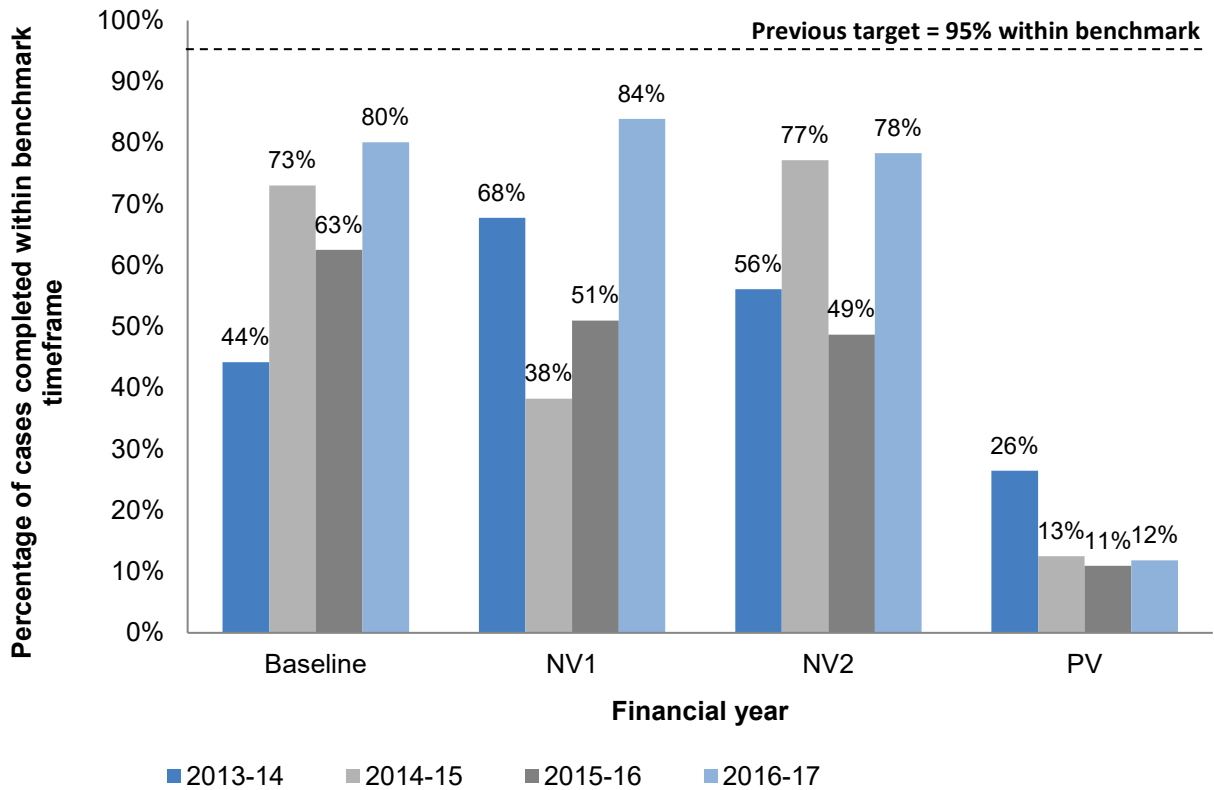
Source: ANAO analysis of AGSVA's reported vetting statistics, 2010–11 to 2016–17

2.70 As a smaller number of clearances take far longer than benchmark timeframes to process, AGSVA's revised indicator (average processing time) is not the most appropriate indicator for clearance timeframes (see Appendix 4 for graphical representations of AGSVA's clearance timeframes in 2016–17, which show skewed distributions).<sup>38</sup> Although AGSVA did not achieve its original 95 per cent performance target, AGSVA's original indicator (percentage of clearance cases completed within benchmark timeframes) is more appropriate. Examining AGSVA's performance using this indicator shows its performance improved during 2016–17 for Baseline, NV1 and NV2 clearances, reaching around 80 per cent for each clearance level. Rather than using average processing time as its performance indicator, AGSVA should seek agreement from its Governance

38 During 2015–16 and 2016–17, the maximum processing times for each clearance level were: 46 months for Baseline; 56 months for NV1; 63 months for NV2; and 61 months for PV. In technical terms, AGSVA's clearance processing times have a highly skewed distribution. As such, median is a more appropriate measure of central tendency than average (or mean).

Board to an appropriate percentile target for completion of clearance cases within benchmark timeframes.

**Figure 2.3: AGSVA performance against benchmark timeframes, 2013–14 to 2016–17<sup>a</sup>**



Note a: AGSVA did not report results against this indicator for 2010–11 to 2012–13.  
 Source: ANAO analysis of AGSVA reported vetting statistics, 2013–14 to 2016–17.

### Positive Vetting remediation

2.71 AGSVA commenced a remediation program for PV clearances in early 2016 due to a mounting backlog of revalidation cases and escalating delays in processing clearances. In a February 2016 brief to the Secretary of Defence, AGSVA noted that the PV backlog was ‘at crisis point’ and it was working with AGD, the Department of the Prime Minister and Cabinet and ASIO to agree and implement remediation actions. In the same brief, AGSVA forecast that it would eliminate its backlog and achieve benchmark clearance timeframes for PV clearances by 2020–21 (see Table 2.8).

**Table 2.8: AGSVA’s forecast PV backlog and processing times, 2015–16 to 2020–21**

Financial year	2015–6	2016–17	2017–18	2018–19	2019–20	2020–21
Forecast backlog size	>2000	1760	450	180	100	0
Forecast processing times (months)	14.3	13.9	7.9	6.8	6.4	6.0

Source: AGSVA brief to Secretary of Defence, February 2016.

2.72 Measures introduced as part of the PV remediation program have included:

- increasing the revalidation period for PV and NV2 security clearances from five to seven years (to provide a two year respite from revalidations);
- decreasing the checkable background period for PV clearances from whole-of-life to 10 years or from 16 years of age, whichever is greater (to reduce vetting effort);
- cooperating with ASIO to reduce the caseload of PV referrals awaiting ASIO security assessment, which totalled around 1100 cases by September 2017;
- increasing vetting resources by adding more PV vetting officers and increasing the pool of contracted psychologists; and
- business process re-engineering aimed at improving prioritisation, allocation and integrated team approaches.

2.73 The *2017 Independent Intelligence Review* conducted by the Department of the Prime Minister and Cabinet noted the impact AGSVA's processing times for PV clearances were having on the intelligence community workforce. It recommended the situation be reviewed again in early 2018, to allow time for the remediation program to have effect, and that alternative options, such as shifting responsibility for PV clearances to ASIO or allowing non-exempt intelligence agencies<sup>39</sup> to conduct their own PV clearances, should be considered if processing times still exceeded six months.<sup>40</sup>

2.74 In September 2017, AGSVA reported to its Governance Board that:

For PV revalidations, the backlog and processing times will likely remain high for another two years. AGSVA is expediting priority revalidations and is actively risk managing delays in revalidations through the annual security appraisal process for all existing PV holders.

2.75 AGSVA's actual backlog size and average processing times for PV clearances over the period 2015–16 to 2017–18 (see Table 2.9) have not declined in line with its February 2016 forecasts (outlined in Table 2.8 above). Partly this has been due to an increasing backlog of clearances awaiting an ASIO security assessment, as ASIO's capacity to complete assessments has not kept pace with AGSVA's increased PV vetting throughput.

**Table 2.9: AGSVA's actual PV backlog and processing times, 2015–16 to 2017–18**

Performance as at	30 June 2016	30 June 2017	18 September 2017
PV backlog size	2306	3581	3206
Average processing times (months)	17.1	17.6	17.8

Source: AGSVA reporting to AGSVA Governance Board

2.76 AGSVA has acknowledged that it will not reduce its PV processing times to under six months by early 2018.

39 Non-exempt Australian Intelligence Community agencies include the Australian Crime and Intelligence Commission, Australian Geospatial-Intelligence Organisation, Australian Signals Directorate, Australian Transactions Reports and Analysis Centre, Defence Intelligence Organisation, Home Affairs and Inspector-General for Intelligence and Security.

40 Commonwealth of Australia, *2017 Independent Intelligence Review*, Department of the Prime Minister and Cabinet, June 2017, pp. 77-8.

## Does AGSVA have comprehensive quality assurance programs for its contractors and internal vetting decisions?

AGSVA has implemented a comprehensive quality audit program for its contractors through its quality management system. It has also introduced periodic internal peer reviews for vetting decisions. It has not instituted a program of independent quality assurance of vetting delegates' decisions.

2.77 ANAO Audit Report No.45 of 2014–15 made two recommendations relating to quality assurance, recommending that Defence:

- implement a targeted audit program to assess Industry Vetting Panel contractors' operations<sup>41</sup>; and
- introduce a program of internal peer review supplemented by periodic independent quality assurance of delegate decisions.<sup>42</sup>

2.78 AGSVA's quality management system, which comprises its vetting policies and procedures, an internal quality audit program and quarterly management reviews, was granted International Standards Organization (ISO) 9001:2008 accreditation in April 2014. It gained reaccreditation under ISO 9001:2015 in May 2017.

2.79 In February 2016, AGSVA commenced a targeted audit program of all current Industry Vetting Panel contractors, which was undertaken in tranches as part of its 2015–16 and 2016–17 internal quality audit program. The audits found contractors were generally conforming in the areas of: staffing, training and professional development; quality control, assurance, monitoring and measuring; and feedback handling, warranty returns and remedial action. However, the audits identified consistent areas of contractor non-conformance and recommended corrective actions to address:

- the use of superseded or obsolete procedural documents;
- uncontrolled records management practices that were non-compliant with information security requirements; and
- failure to undertake security awareness training and maintain local security policies and procedures.

2.80 Also in February 2016, AGSVA established an internal peer review program, involving the review by vetting supervisors of a random selection of 'grant' decisions for each clearance level (42 for Baseline, 42 for NV1, 21 for NV2 and 10 for PV) every six months. As at November 2017, three peer review rounds had been completed for the Baseline, NV1 and NV2 clearance levels, with the majority of cases being assessed as compliant. For all cases that were assessed as non-compliant, the reviewer determined that the compliance issue had no bearing on the vetting decision. One PV round of peer review has been completed (in July-August 2017), with all cases being assessed as compliant.

---

41 ANAO Audit Report No.45 2014–15 *Central Administration of Security Vetting*, p. 70.

42 *ibid.*, p. 78.

2.81 AGSVA wrote to ASIO and the Department of Foreign Affairs and Trade (two authorised vetting agencies) in September 2015, and held subsequent meetings with these entities, gaining in-principle agreement to undertake six-monthly external peer review of a selection of NV1, NV2 and PV 'grant' decisions. However, AGSVA was not able to provide evidence that this external peer review program had been implemented. AGSVA should establish an independent quality assurance process for vetting delegates' decisions, in line with the ANAO's recommendation in the previous audit.

### 3. Entity compliance with personnel security requirements

---

#### Areas examined

The ANAO assessed selected entities' compliance with Protective Security Policy Framework (PSPF) requirements related to personnel security, including communication with the Australian Government Security Vetting Agency (AGSVA). The entities assessed were Attorney-General's Department (AGD), Australian Radiation Protection and Nuclear Safety Authority (ARPANSA), Australian Securities and Investments Commission (ASIC), Department of Home Affairs (Home Affairs) and Digital Transformation Agency (DTA).<sup>43</sup>

#### Conclusion

Selected entities' compliance with PSPF personnel security requirements was mixed. While most entities had policies and procedures in place for personnel security, some entities were only partially compliant with the PSPF requirements to ensure personnel have appropriate clearances. None of the entities had fully implemented the PSPF requirements introduced in 2014 relating to managing ongoing suitability. In addition, entities did not always notify AGSVA when clearance holders leave the entity.

#### Areas for improvement

The ANAO made five recommendations aimed at ensuring entities: have appropriate risk-based personnel security practices; implement quality assurance mechanisms to reconcile their personnel records with AGSVA's clearance holder records; comply with eligibility waiver requirements; and undertake an annual health check for clearance holders and their managers.

#### Do entities have appropriate risk-based policies, plans and procedures for personnel security?

AGD, ARPANSA, ASIC and Home Affairs had plans, policies and procedures in place for personnel security. In some cases, these documents had not been updated to reflect 2014 revisions to PSPF personnel security requirements. DTA had not finalised any of these documents. There was limited evidence of entities undertaking personnel security risk assessments to inform their plans, policies and procedures.

3.1 Under the governance requirements of the PSPF, entities must:

- prepare a protective security plan, updated at least every two years (GOV-4);
- develop a set of protective security policies and procedures (GOV-5); and
- adopt a risk management approach to protective security (GOV-6).<sup>44</sup>

---



































43 During the course of the audit, as a result of a machinery of government change, the Department of Immigration and Border Protection became the Department of Home Affairs, incorporating national security and law enforcement policy and operations. For clarity, all references in this report are to its current name.

44 See Appendix 2 for a list of PSPF governance (GOV) requirements related to personnel security.



3.2 AGD, ARPANSA, ASIC and Home Affairs were able to produce cleared documentation regarding these requirements. DTA, which was established as a non-corporate Commonwealth entity in July 2015, had not finalised a protective security plan, policies or a risk assessment. Table 3.1 shows a summary of entity performance against the PSPF requirements and recommended practices, with a focus on whether entities are effectively planning, developing policies and procedures and undertaking risk assessment for personnel security.

**Table 3.1: Entity security plans, policies, procedures and risk assessments**

	AGD	ARPANSA	ASIC	Home Affairs	DTA
Had the entity undertaken regular security planning with adequate oversight and consultation?					
Did the security plan adequately cover personnel security?					
Were policies and procedures current, accessible and subject to adequate oversight and review?					
Did policies and procedures adequately cover personnel security?					
Had the entity recently undertaken a protective security risk assessment?					
Had personnel security been considered as part of security risk management?					
Key:  Not Met: Did not satisfy any of the considerations for the criterion.  Partly Met: Satisfied some (less than 65%) of the considerations.  Mostly Met: Satisfied most (65% or more) of the considerations.  Met: Satisfied all of the considerations.					

Source: ANAO analysis of entity documentation based on criteria outlined at Appendix 5.

3.3 AGD, ARPANSA, ASIC and Home Affairs had completed a protective security plan to manage their security risks. Three entities, AGD, ARPANSA and Home Affairs, had not updated or revised their plans at least every two years as required.<sup>45</sup> The quality of plans varied between agencies, with some entities' plans containing few measures or actions relating to personnel security. Where measures or actions had been identified, detail was often lacking with regard to responsibility for implementation, intended outcomes or performance indicators. DTA has a draft security plan, which it expected to finalise in the second half of 2017–18.

<sup>45</sup> AGD and ARPANSA had current plans in place, but their previous plans had been finalised more than two years prior. Home Affairs' plan was dated 14 July 2015, more than two years prior to the ANAO's assessment; it had commenced but not completed the development of a replacement plan.

3.4 All entities had some level of personnel security policies and procedures in place and accessible on their intranet sites. In many cases, policies and procedures had not been kept up-to-date or updated to reflect recent changes to the PSPF. Home Affairs had the most comprehensive suite of policies, procedures and instructions for personnel security. While DTA had limited procedural documentation on its intranet, it did not have any formal protective security policies; it had developed draft protocols for physical and information security, but not for personnel security.

3.5 Selected entities had generally identified trusted insiders as a key threat, but their protective security risk assessments focussed on physical and information security. ARPANSA, ASIC and Home Affairs had undertaken protective security risk assessments within the past two years, which considered personnel security. AGD's most recent risk assessment, finalised in June 2015, did not consider personnel security. DTA advised that it had conducted an initial security risk assessment in 2015, but could not provide evidence. ARPANSA was the only entity that had recently conducted a personnel security risk assessment.

#### Recommendation no.4

3.6 The Attorney-General's Department and the Digital Transformation Agency conduct a personnel security risk assessment that considers whether changes are needed to their protective security practices.

**Attorney-General's Department's response:** *Agreed.*

3.7 *The department previously engaged an external Risk Assessment consultant prior to the announcement of the machinery of government changes in 2017. This was put on hold to be reinitiated after the machinery of government changes were completed as our expectation was that these changes would have a significant impact on our security risk profile. The department is currently working with the consultant on the new terms of reference for the personnel and physical risk assessment to align with the new organisational structure.*

**Digital Transformation Agency's response:** *Agreed.*

3.8 *The DTA is currently is in the process of developing the DTA security plan and the protective and personal security policies. The DTA acknowledges that this is an immediate action and implementation.*

#### Recommendation no.5

3.9 The Digital Transformation Agency take immediate action to comply with the Protective Security Policy Framework governance requirements.

**Digital Transformation Agency's response:** *Agreed.*

3.10 *The DTA is currently is in the process of developing the DTA security plan and the protective and personal security policies. The DTA acknowledges that this is an immediate action and implementation.*

3.11 The 2016 Belcher Review recommended revisions to PSPF governance requirements ‘to streamline requirements and remove duplication with other requirements imposed on entities’ and ‘improve communication and support to entities to implement the PSPF, in particular to assist entities adopt a sound risk-based approach’.<sup>46</sup> At the time of conducting this audit, AGD was making revisions to the PSPF in light of these recommendations, with a target date for changes to the PSPF to come into effect on 1 July 2018.

3.12 Selected entities were slow to adopt changes to the PSPF requirements within their plans, policies and procedures. This suggests entities could benefit from simpler and more streamlined policy requirements and greater support from AGD as policy owner. Potential support could include provision of templates for components such as security plans and risk assessments, and dissemination of better practice examples.

### Do entities assess the eligibility and suitability of personnel to access government resources?

AGD, ASIC, Home Affairs and DTA did not have adequate controls and quality assurance mechanisms for ensuring their personnel have appropriate clearances. For each of these entities, a small number of current personnel were identified who did not hold required clearances. Employment screening processes varied across the selected entities. AGD, ASIC and Home Affairs had higher denial rates than AGSVA and made greater use of aftercare.

3.13 Under the personnel security requirements of the PSPF, entities must:

- ensure the eligibility and suitability of their personnel to access Australian Government resources, through conducting effective employment screening (PERSEC-1);
- identify, record and review positions that require a security clearance (PERSEC-2); and
- ensure personnel accessing classified resources have a security clearance from AGSVA<sup>47</sup> at an appropriate level (PERSEC-4 and PERSEC-6).<sup>48</sup>

### Employment screening

3.14 The purpose of employment screening is to provide entities with assurance that their personnel are eligible and suitable to be granted access to Australian Government resources. Employment screening generally occurs prior to engagement and involves confirming an individual’s identity, checking their integrity and reliability, and obtaining signed declarations (such as a confidentiality and non-disclosure agreement or ‘official secrets’ declaration).

3.15 Based on entity practices, prospective employees or contractors undergoing employment screening are:

- (a) granted employment;

<sup>46</sup> Barbara Belcher, *Independent Review of Whole-of-Government Internal Regulation—Report to the Secretaries Committee on Transformation*, volume 1, Canberra, August 2015, p. 40.

<sup>47</sup> Unless the entity is an authorised vetting agency.

<sup>48</sup> See Appendix 2 for a list of PSPF personnel security (PERSEC) requirements.

- (b) granted employment subject to aftercare arrangements (such as periodic reporting relating to suitability concerns, or restrictions on duties or access); or
- (c) denied employment due to identified eligibility or suitability concerns.

3.16 The PSPF guidelines *Agency personnel security responsibilities* recommend entities assess the integrity and reliability of personnel by considering character traits and behaviours such as honesty, maturity, trustworthiness, loyalty, tolerance and resilience. Entities should also determine if personnel may be vulnerable to improper influence, by assessing potential conflicts of interest and membership of relevant issue motivated groups.

3.17 Statistics on employment screening processes undertaken by each entity during 2015–16 and 2016–17 and the outcomes of those screening process are in Table 3.2 (with the exception of DTA, which could only provide statistics from April 2017, due to inadequate records).

**Table 3.2: Entity employment screening statistics, 2015–16 and 2016–17**

Entity	Financial year	Screening processes completed	Screening outcomes			
			Granted	Granted with aftercare	Denied	Denial rate
<b>AGD</b>	2015–16	895	891	0	4	0.45%
	2016–17	797	790	2	5	0.63%
<b>ARPANSA</b>	2015–16	28	28	0	0	-
	2016–17	23	23	0	0	-
<b>ASIC</b>	2015–16	634	625	8	1	0.16%
	2016–17	578	548	27	3	0.52%
<b>Home Affairs</b>	2015–16	2195	2167	11	17	0.77%
	2016–17	2943	2898	17	28	0.95%

Source: AGD, ARPANSA, ASIC and Home Affairs.

3.18 Only the three larger entities, AGD, ASIC and Home Affairs, had denied individuals access due to suitability concerns and used aftercare arrangements over this period. While these entities’ denial rates were low (less than one per cent), they were higher than AGSVA’s denial rates for Baseline clearances over the same period (0.01 per cent in 2015–16 and 0.04 per cent in 2016–17). In addition, these larger entities have shown a willingness to use aftercare arrangements in circumstances where they determined that suitability concerns could be mitigated. In contrast, AGSVA did not impose clearance maintenance requirements (or aftercare) for any of the 38,713 Baseline clearances it granted during 2015–16 and 2016–17 (see Chapter 2 for further discussion of AGSVA’s clearance denial rate and use of aftercare).

3.19 The ANAO assessed the extent to which: employment screening practices within selected entities complied with mandatory controls and recommended practices outlined in PSPF policy documents (see Table 3.3); and involved recommended screening checks (see Table 3.4).

**Table 3.3: Entity employment screening practices<sup>a</sup>**

	AGD	ARPANSA	ASIC	Home Affairs	DTA
<b>Record results of screening<sup>a</sup></b>	✓	✓	✓	✓	✗
<b>Consent to collect information</b>	✓	✓	✓	✓	✓
<b>Consent to share information</b>	✗	✗	✓	✓	✗
Official secrets declaration	✗ <sub>b</sub>	✓	✓	✓	✓
Statutory declaration	✗ <sub>b</sub>	✓	✗	✓	✓

Note a: Practices in bold print are mandatory controls.

Note b: AGD used two screening packs over this period; each pack contained one declaration but not the other.

Source: ANAO analysis of entity documentation.

3.20 DTA was not fully compliant with the PSPF mandatory control (associated with PERSEC-1) that 'Agencies **are to** record the results of the employment screening for successful applicants and any additional agency specific screening relating to each person'.<sup>49</sup> DTA should establish procedures for recording the results of its employment screening.

3.21 AGD, ARPANSA and DTA had not updated the consent forms in their employment screening packs to obtain informed consent from individuals to share personal information with other entities, including AGSVA (this relates to the PERSEC-8 requirement to share relevant information with AGSVA, discussed later in this chapter).

49 AGD, *Australian Government Personnel Security Protocol*, version 2.1, Canberra, April 2015, p. 11. Emphasis in original.

**Table 3.4: Entity employment screening checks<sup>a</sup>**

	AGD	ARPANSA	ASIC	Home Affairs	DTA
<b>Mandatory requirement for employment screening</b>					
Identity check	✓	✓	✓	✓	✓
<b>Recommended checks under <i>Australian Standard 4811–2006: Employment Screening</i></b>					
Five year residency check	✗	✓	✓	✓	✗
Five year employment check	✗	✓	✓	✗	✗
Police records check	✓	✓	✓	✓	✓
Professional referee check	✓	✓	✓	✗ <sub>a</sub>	✓
Personal character reference	✗	✓	✓	✗	✓
Qualification verification	✗	✗ <sub>a</sub>	✓	✗ <sub>a</sub>	✗
<b>Additional checks</b>					
Suitability questionnaire	✓	✓	✓	✓	✓
Digital footprint check	✗	✗	✓	✓	✗
ASIC directorship search	✗	✗	✓	✓	✗
Financial history check	✗	✗	✓	✗	✗
Bankruptcy search	✗	✗	✓	✗	✗
Criminal intelligence check	✗	✗	✗	✓	✗

Note a: ARPANSA and Home Affairs advised that, while these checks are not conducted as part of its employment screening process, they form a component of its standard recruitment process.

Source: ANAO analysis of entity documentation.

3.22 All entities met the minimum requirement to undertake an identity check. At the time of assessment, only ASIC conducted all of the checks recommended under *Australian Standard 4811–2006: Employment Screening*. ASIC and Home Affairs undertook additional checks, such as digital footprint and company directorship checks, due to their individual risk profiles.<sup>50</sup>

3.23 In October 2016, in response to the Belcher Review recommendation to reduce duplication between employment screening and Baseline clearances, the Government agreed that entities that conduct employment screening to an equivalent standard could be accredited to issue Baseline clearances to their personnel. AGD is developing an accreditation process, which is expected to come into effect from mid-2018.

<sup>50</sup> A digital footprint check involves checking individuals' publically available online information; for example, information on social networking sites such as Facebook and LinkedIn.

## Identifying and recording clearance requirements

3.24 Under the PSPF, entities are required to maintain a register of positions requiring security clearances and assess clearance requirements before advertising a position, including recording a reason and reassessment date for the requirement. The ANAO examined whether selected entities met these requirements (see Table 3.5).

**Table 3.5: Entity methods of identifying and recording clearance requirements**

	AGD	ARPANSA	ASIC	Home Affairs	DTA
Did the entity have a minimum clearance requirement?	Yes (Baseline)	No	Yes (NV1)	Yes (Baseline)	Yes (Baseline)
What is the rationale for the minimum requirement?	Access to network	-	Assurance	Access to network	Access to network
<b>Did the entity maintain a register of positions requiring clearances?<sup>a</sup></b>	✓	✓	✓	✓	✗
<b>Before advertising a position, did the entity review clearance requirements?</b>	✓	✓	✓	✓	✗
<b>Did the entity record reasons for clearance requirements and reassessment dates?</b>	✗	✗	✗	✗ <sup>b</sup>	✗

Note a: Practices in bold print are mandatory controls.

Note b: Home Affairs records the reasons for PV clearance requirements.

Source: ANAO analysis of entity documentation.

3.25 Four entities had a minimum security clearance requirement for all personnel. This was generally due to the entities' ICT networks being rated at a 'Protected' level, which means personnel accessing their networks would have access to material at this classification level.

3.26 DTA was non-compliant with the PSPF mandatory control (associated with PERSEC-3) that 'Agencies **are to** maintain a register of positions that require a clearance'.<sup>51</sup> In its 2016–17 PSPF compliance report, DTA noted that it was developing a register for endorsement by its Chief Executive Officer. Other entities maintained registers of security clearance requirements.

3.27 AGD, ARPANSA, ASIC and Home Affairs required managers to specify clearance requirements on their recruitment forms, but they did not record a reason and reassessment date for clearance requirements. DTA did not have a recruitment form (approval to recruit was managed through an email exchange) and its internal procedures did not include an instruction for hiring managers to identify clearance requirements as part of the approval process.

## Ensuring personnel accessing classified resources have security clearances

3.28 The ANAO obtained personnel records from selected entities' human resources management information systems and analysed whether personnel engaged in positions that

51 AGD, *Personnel security guidelines—Agency personnel security responsibilities*, version 1.1, Canberra, April 2015, p. 34. Emphasis in original.

required security clearances, as at 11 September 2017, had active clearances with AGSVA. As entities and AGSVA did not consistently use a common identifier across their datasets, the ANAO developed a methodology to match entity personnel to an associated AGSVA clearance using basic biographical data (see Appendix 6 for an explanation of the methodology and its limitations).

3.29 ARPANSA operates an ‘Unclassified’ network, so not all of its personnel require a security clearance. The ANAO’s examination of ARPANSA’s records established that all ARPANSA personnel who required a clearance, as at 11 September 2017, had corresponding active clearance records in AGSVA’s database.

3.30 As noted in Table 3.5 above, AGD, ASIC, Home Affairs and DTA have minimum security clearance requirements for all personnel. Currently engaged personnel within these entities should have an active clearance recorded in AGSVA’s database. The results of the ANAO’s matching analysis for these entities are outlined in Table 3.6.

**Table 3.6: ANAO matching of entity personnel records with AGSVA clearance records, as at 11 September 2017**

Entity	Number of personnel engaged at entity	Confidence of match <sup>a</sup>	Count of matches with active AGSVA clearances	Percentage of personnel matched at confidence level
<b>AGD</b>	2366	High	2222	93.91%
		Medium	43	1.82%
		Low	25	1.06%
		No match <sup>b</sup>	76	3.21%
<b>ASIC</b>	2534	High	1846	72.85%
		Medium	81	3.20%
		Low	82	3.24%
		No match <sup>b</sup>	525	20.72%
<b>Home Affairs</b>	19260	High	17903	92.95%
		Medium	602	3.13%
		Low	275	1.43%
		No match <sup>b</sup>	480	2.49%
<b>DTA</b>	210	High	189	90.00%
		Medium	5	2.38%
		Low	8	3.81%
		No match <sup>b</sup>	8	3.81%

Note a: See Appendix 6 for an explanation of the matching confidence levels.

Note b: ‘No match’ indicates that the ANAO could not identify a matching AGSVA clearance record.

Source: ANAO analysis of entity personnel records and AGSVA clearance data.



3.31 Entities advised the ANAO of explanations for these discrepancies in the matching of clearance records including:

- entities failing to promptly sponsor or re-sponsor a clearance when cleared personnel transferred between entities (meaning the clearance became inactive);
- personnel recorded on the human resources management information system who did not require a clearance or had an active clearance with an exempt agency;
- personnel having been granted clearances prior to the establishment of AGSVA that were still within their revalidation period but had not uploaded to AGSVA's database;
- personnel not complying with AGSVA's revalidation process and having their clearances cancelled without informing the security office;
- personnel not advising AGSVA of name changes (for example, due to marriage);
- entities' personnel records were inaccurate (for example, an individual's name or date of birth incorrectly recorded); and
- in one case, an employee was on long-term leave when an entity's minimum clearance requirement changed and the need for a clearance was not identified on their return.

3.32 In the case of ASIC, its security office had formed an incorrect view that its internal employment screening process was sufficient to allow access to 'Protected' material. Of the 525 ASIC personnel in the 'no match' category, 464 were recorded in ASIC's personnel database as having only undergone ASIC's pre-employment screening. In August 2017, in its 2016–17 PSPF compliance report, ASIC advised its minister that:

The ASIC PeopleSoft database indicates 1527 ASIC employees and contractors hold a National Security Clearance of Baseline, Highly Protected, [NV1] or [NV2]. An additional 1008 ASIC employees and or contractors are shown as only holding an ASIC Pre-engagement Assessment ... ASIC appears to have not previously submitted requests to the AGSVA for the granting of temporary or provisional access to classified information... Consequently, a limited number of ASIC employees or contractor may have access to the SharePoint document management system and documents classified as PROTECTED or have the opportunity to oversight printed material classified at PROTECTED or above.

3.33 ASIC now provides applicants with a letter advising that its assessment only allows access to unclassified information.

3.34 For AGD, Home Affairs and DTA, many personnel identified in the 'no match' category either held active security clearances (which could not be matched due to typographical errors with biographical data) or had previously held clearances that could be reinstated. Nevertheless, for each of these entities the ANAO's analysis identified a small number of current personnel who required a security clearance but did not hold one.

3.35 AGD, ASIC, Home Affairs and DTA were consequently partially compliant with the PERSEC-4 requirement to ensure all personnel accessing classified resources have a security clearance at an appropriate level. ASIC was also partially compliant with the PERSEC-6

requirement to use AGSVA to conduct vetting, as in certain cases it had been providing permission to access classified material on the basis of its own internal employment screening.<sup>52</sup>

3.36 The four partially compliant entities did not have adequate controls and quality assurance mechanisms for ensuring their personnel have appropriate clearances. At a minimum, entities should record clearance levels, revalidation dates and clearance subject identifiers for all personnel with an active security clearance, and regularly reconcile these records with AGSVA's records of the clearances they actively sponsor.

## Recommendation no.6

3.37 The Attorney-General's Department, the Australian Securities and Investments Commission, the Department of Home Affairs and the Digital Transformation Agency implement quality assurance mechanisms to reconcile their personnel records with AGSVA's clearance holder records, and commence clearance processes for any personnel who do not hold a required clearance.

**Attorney-General's Department's response:** *Agreed.*

3.38 *The department has recently concluded a full review of all its clearance holder records and can confirm that all staff either hold the required clearance or have commenced the security clearance process. We are in the process of transferring and/or cancelling sponsorship of clearances that should no longer be sponsored by the department. Going forward, the department will conduct an annual review of clearance holder records to ensure the accuracy of our records.*

**Australian Securities and Investments Commission's response:** *Agreed.*

**Department of Home Affairs' response:** *Agreed.*

3.39 *The Department agrees to implement further quality assurance mechanisms and include periodic checking of data against AGSVA's clearance holder records. The Department is reviewing its records to identify any personnel without a current security clearance that require an AGSVA clearance. The Department will ensure clearance packs are issued and submitted.*

**Digital Transformation Agency's response:** *Agreed.*

3.40 *The DTA will implement a schedule to ensure that there is a regular (no longer than a six-month period) audit of the Australian Government Security Vetting Agency (AGSVA) clearances held by the DTA and the DTA personnel records.*

3.41 *The DTA's Customer Relationship Manager (CRM) will assist to keep track of all employees and contractors to ensure that they have the appropriate clearance for their role in the Agency. This will ensure that every staff member, contractor and consultant that is engaged will be subject to the DTA onboarding process. The CRM will also ensure that when a person separates from the Agency that their clearance is no longer sponsored by the DTA.*

---

52 At the completion of employment screening, ASIC issued commencing personnel with a letter stating that its employment screening assessment 'permits access to ASIC's information classified up to and including the level of PROTECTED'.

## Are entities identifying and appropriately mitigating business impacts resulting from security clearance requirements?

All entities used the temporary access or eligibility waiver provisions of the PSPF to mitigate business impacts resulting from the timeframes to obtain, and eligibility requirements for, security clearances. AGD and Home Affairs used temporary access provisions appropriately to mitigate delays in onboarding personnel. AGD, ARPANSA, ASIC and DTA had not fully complied with PSPF controls for eligibility waivers.

3.42 As discussed in Chapter 2, it can take several months (and in some cases years) for AGSVA to process a security clearance, depending on the level of clearance and complexity of the case. These timeframes can have a significant impact on entities' business activities, due to potential delays in onboarding personnel.<sup>53</sup>

3.43 Under the PSPF, there are two mechanisms that entities can use to mitigate business impacts resulting from clearance requirements:

- temporary access—which allows entities to provide personnel with access to classified material on a short-term (up to three months, prior to applying for a clearance) or provisional (for the duration of the clearance process) basis; and
- eligibility waivers—which allow entities to waive citizenship and checkable background requirements for security clearances where there is an exceptional business case.

3.44 For all temporary access and eligibility waivers, entities are required to conduct detailed risk assessments, gain approval from the accountable authority (or a delegate) and consult AGSVA.<sup>54</sup> Eligibility waivers must be reassessed annually. The ANAO examined whether selected entities met temporary access and eligibility waiver requirements; the results of this testing are in Table 3.7 and Table 3.8.

---

53 For example, the Inspector-General of Intelligence and Security has noted the impact of extended wait times for PV clearances on her office's recruitment activity. Parliamentary Committee on Intelligence and Security, *Review of Administration and Expenditure No. 15 (2015-2016) – Australian Intelligence Agencies*, Canberra, June 2017, p. 42.

54 For provisional access requests, AGSVA undertakes a preliminary assessment and provides a risk advisory notice if it identifies any potential security concerns (see paragraph 2.39).

**Table 3.7: Selected entities' use of temporary access<sup>a</sup>**

	AGD	ARPANSA	ASIC	Home Affairs	DTA
Short-term access, 2016–17	116	0	0	257	0
Provisional access, 2016–17	64	0	0	68	0
<b>Did the entity conduct risk assessments?<sup>a</sup></b>	✓	-	-	✓	-
<b>Did the entity gain accountable authority or delegate approval?</b>	✓	-	-	✓	-
<b>Did the entity consult AGSVA?</b>	✓	-	-	✓	-

Note a: Practices in bold print are mandatory controls.

Source: ANAO analysis of entity and AGSVA documentation.

3.45 Two entities, AGD and Home Affairs, that made regular use of temporary access during 2016–17 maintained registers of temporary access granted, had procedures in place to conduct risk assessments and consulted AGSVA on any potential security concerns. AGD and Home Affairs had delegation instruments in place and gained delegate approval for temporary access.

**Table 3.8: Selected entities' use of eligibility waivers<sup>a</sup>**

	AGD	ARPANSA	ASIC	Home Affairs	DTA
Eligibility waivers, 2015–16	3	3	unknown <sup>b</sup>	6	unknown <sup>c</sup>
Eligibility waivers, 2016–17	2	4	unknown <sup>b</sup>	6	unknown <sup>c</sup>
<b>Did the entity conduct risk assessments?<sup>a</sup></b>	✓	✓	✗	✓	✓
<b>Did the entity gain accountable authority or delegate approval?</b>	✓	✓	✗	✓	✗
<b>Did the entity reassess eligibility waivers annually?</b>	✗	✗	✗	✓	✗

Note a: Practices in bold print are mandatory controls.

Note b: ASIC reported in 2016–17 that it had engaged 120 non-citizens without a security clearance or eligibility waiver in place.

Note c: DTA did not maintain adequate records of its eligibility waivers.

Source: ANAO analysis of entity and AGSVA documentation.

3.46 All entities had engaged personnel with security clearances subject to eligibility waivers during 2015–16 and 2016–17. However, Home Affairs was the only entity that was fully compliant with PSPF mandatory controls relating to eligibility waivers (associated with PERSEC-5).

- AGD, ARPANSA, ASIC and DTA could not provide evidence that they were compliant with the mandatory control that 'Agencies **are to** reassess eligibility waivers yearly'.<sup>55</sup>

55 AGD, *Australian Government Personnel Security Protocol*, version 2.1, Canberra, April 2015, p. 21. Emphasis in original.

- Managers in DTA had approved eligibility waivers without a delegation from the accountable authority.
- ASIC advised in its 2016–17 PSPF compliance report that it had issued 120 ‘internal citizenship waivers’ to non-Australian citizens, some of whom had been given access to its ‘Protected’ network without an appropriate security clearance.

### Recommendation no.7

3.47 The Attorney-General’s Department, the Australian Radiation Protection and Nuclear Safety Authority, the Australian Securities and Investments Commission and the Digital Transformation Agency review their policies and procedures for eligibility waivers to ensure they are compliant with Protective Security Policy Framework mandatory controls.

**Attorney-General’s Department’s response:** *Agreed.*

3.48 *The department has implemented an ICT solution where eligibility waivers are stored and information relating to the waiver is documented. This will ensure we can access the relevant information immediately and support the annual reassessment of all waivers, in accordance with PSPF requirements.*

**Australian Radiation Protection and Nuclear Safety Authority’s response:** *Agreed.*

3.49 *ARPANSA has updated our policy and procedures to reflect the requirement to undertake risk assessments every year for those who have been granted an eligibility waiver.*

**Australian Securities and Investments Commission’s response:** *Agreed.*

**Digital Transformation Agency’s response:** *Agreed.*

3.50 *The DTA is currently developing the DTA security plan and the protective and personal security policies for approval. The procedures for eligibility waivers will be included in this review. The DTA acknowledges that this is an immediate action and implementation.*

### Do entities manage the ongoing suitability of personnel to access government resources?

AGD, ARPANSA, ASIC and Home Affairs had accessible policies and procedures for managing ongoing suitability, including change of circumstances and contact reporting, and mandatory security awareness training that covered personnel security requirements. DTA had not established these arrangements, as required under the PSPF. None of the entities had implemented the PSPF requirement to conduct an annual health check for clearance holders and their managers.

3.51 Under the personnel security requirements of the PSPF, entities must establish and implement policies and procedures to assess and manage the ongoing employment suitability of their personnel (PERSEC-2) and for security clearance maintenance (PERSEC-7). Key measures identified in PSPF policy documents relating to these requirements include:

- provision of security awareness training to personnel;
- undertaking periodic suitability checks, based on entity-specific risk factors<sup>56</sup>;
- requiring clearance holders to report changes in personal circumstances to the entity security office and AGSVA;
- requiring personnel to report suspicious, on-going, unusual or persistent contacts with foreign officials and other foreign nationals to the entity security office;
- conducting an annual ‘health check’ process for clearance holders and their managers.

**Table 3.9: Entity arrangements for ongoing suitability and clearance maintenance<sup>a</sup>**

	AGD	ARPANSA	ASIC	Home Affairs	DTA
<b>Ongoing suitability</b>					
<b>Did the entity’s security training cover personnel security?<sup>a</sup></b>	✓	✓	✓	✓	✗
Did the entity undertake periodic suitability checks of personnel?	✗	✗	✗	✓	✗
<b>Clearance maintenance</b>					
<b>Did the entity have policies and procedures for change of circumstance reporting?</b>	✓	✓	✓	✓	✗
<b>Did the entity have policies and procedures for contact reporting?</b>	✓	✓	✓	✓	✗
<b>Did the entity undertake an annual health check?</b>	✗	✗	✗	✗	✗

Note a: Practices in bold print are mandatory controls.

Source: ANAO analysis of entity documentation.

3.52 AGD, ARPANSA, ASIC and Home Affairs had developed security awareness eLearning packages, which were mandatory for all personnel and included adequate coverage of personnel security requirements. Home Affairs was the only entity that had implemented periodic suitability checks of its personnel based on its risk profile.

3.53 DTA was non-compliant with the PERSEC-2 requirement to implement ongoing suitability policies and procedures. At the time of conducting this audit, DTA had not established a security awareness training program; its security training consisted of an informal discussion with commencing personnel as part of their induction into the entity. DTA was also non-compliant with

<sup>56</sup> This is a recommended action, not a mandatory control.

the PERSEC-7 requirement to establish and implement policies and procedures for security clearance maintenance. In implementing Recommendation no.5 (paragraph 3.9), DTA should address these areas of non-compliance.

3.54 The other four entities had policies and procedures on change of circumstances and contact reporting, which were available to their personnel on their intranet sites. However, all five entities were non-compliant with the annual health check requirement, outlined in the following PSPF mandatory control (associated with PERSEC-7):

Agencies **are to** annually require:

- clearance holders to confirm they have reported to their agency security section:
  - all changes of circumstances; and
  - any suspicious, on-going, unusual or persistent contacts;
- clearance holders to complete any required security awareness training; and
- managers responsible for personnel to confirm they have reported any concerns about the clearance holders.<sup>57</sup>

---

57 AGD, *Personnel security guidelines—Agency personnel security responsibilities*, version 1.1, Canberra, April 2015, p. 38. Emphasis in original.

## Recommendation no.8

3.55 The Attorney-General's Department, the Australian Radiation Protection and Nuclear Safety Authority, the Australian Securities and Investments Commission, the Department of Home Affairs and the Digital Transformation Agency implement the Protective Security Policy Framework requirement to undertake an annual health check for clearance holders and their managers.

**Attorney-General's Department's response:** *Agreed.*

3.56 *The department is developing options for a new process to implement a yearly health check including to align with the Program for Performance Improvement process which occurs 30 June every year.*

**Australian Radiation Protection and Nuclear Safety Authority's response:** *Agreed.*

3.57 *Following the security risk assessment conducted in June 2017 by the Agency Security Group, the annual health check was firmly placed in the 2017/18 FY program of works. Consultation and coordination efforts with ARPANSA's People and Culture has occurred since that time to design and implement the health checks in a manner that is consistent with the agency's people management program. As such the health checks are expected to roll out within the 2018 calendar year.*

**Australian Securities and Investments Commission's response:** *Agreed.*

**Department of Home Affairs' response:** *Agreed.*

3.58 *The Department will introduce an annual health check for managers, noting revisions to the PSPF are expected; and will implement this process once those changes are confirmed and AGD guidelines are published.*

**Digital Transformation Agency's response:** *Agreed.*

3.59 *The DTA will implement the PSPF requirement for and annual health check for all clearance holders and their managers. The DTA will commence this process by 31 July to allow for the proposed changes to the PSPF, which are due to come into effect on 1 July 2018.*

## Do entities share relevant information with AGSVA?

All entities were partially compliant with the PSPF requirement to inform AGSVA when security cleared personnel leave the entity. AGD, ARPANSA and DTA had not updated their employment screening forms to obtain informed consent from personnel to share sensitive information with AGSVA.

3.60 Under the personnel security requirements of the PSPF, entities and vetting agencies must share information that may impact on an individual's ongoing suitability to hold a clearance (PERSEC-8) and entities must have policies and procedures to notify vetting agencies of clearance holder staff separations and any resulting security concerns (PERSEC-9).



## Sharing information on ongoing suitability

3.61 Entity security offices are required to report any information on clearance holders of potential interest to AGSVA (such as travel to countries of concern, disciplinary actions, security breaches or concerns identified through screening). To support entity-initiated disclosure, the PSPF includes a mandatory control (associated with PERSEC-8) that:

Agencies **are to** obtain written consent from all clearance subjects (existing and potential) to share information with other agencies for the purposes of assessing their initial and ongoing suitability to access Australian Government resources.<sup>58</sup>

3.62 As noted in paragraph 3.21, AGD, ARPANSA and DTA had not updated their employment screening consent forms to explicitly obtain informed consent to share personal information, including sensitive information, with other entities such as AGSVA. These entities were non-compliant with the mandatory control.

## Advising AGSVA of clearance holder separations

3.63 Analysis of AGSVA's clearance records and entity personnel records indicates that the number of active clearances sponsored by entities exceeds entities' staffing profiles (see Table 3.10 below). While there are various factors that may contribute to this variance (such as entities sponsoring clearances for other parties, or data quality issues with entity personnel records), the large disparities suggest entities are not promptly notifying AGSVA of all personnel separations. This reduces the assurance available to these entities that their personnel are properly cleared. It also reduces the assurance available to AGSVA that its clearance records are complete and accurate.<sup>59</sup>

**Table 3.10: Comparison of entity personnel and clearance holder profiles, as at 11 September 2017**

	AGD	ARPANSA	ASIC	Home Affairs	DTA
Number of engaged personnel <sup>a</sup>	2366	148	2534	19260	210
Sponsored security clearances	4762	180	2841	36032	330
Clearances as percentage of engaged personnel	201%	122%	112%	187%	157%

Note a: Includes all personnel types (non-ongoing staff, contractors and secondments); except for DTA who could not provide sufficient biographical data for contractors.

Source: ANAO analysis of entity personnel records and AGSVA clearance data.

3.64 AGD, ARPANSA, ASIC and Home Affairs had separation policies and procedures in place that included notifying the security office of separations and required separating personnel to complete a 'Declaration of Secrecy on Cessation of Duties' form. In late 2017, AGD automated these processes within its human resources management information system; whereas ARPANSA,

58 *ibid.*, p. 15. Emphasis in original.

59 The ANAO also identified 2238 probable duplicate clearance identities in AGSVA's clearance records. Of these, 1742 were sponsored by Home Affairs, one by AGD and one by ASIC. Home Affairs advised the ANAO that it attributes some of its duplicate clearance identities to a historic issue with dates of birth for clearance holders being inverted.

ASIC and Home Affairs relied on separating personnel completing a cessation checklist. At the time of assessment, DTA did not have any formal separation policies and procedures in place, and was non-compliant with the PERSEC-9 mandatory requirement.

3.65 Despite four entities having procedures in place, the ANAO found 3917 personnel who had separated from selected entities during 2015–16 and 2016–17 and still had active clearances sponsored by those entities as at 11 September 2017 (see Table 3.11).

**Table 3.11: Separated personnel from 2015–16 and 2016–17 with clearances still actively sponsored by selected entities as at 11 September 2017**

	AGD	ARPANSA	ASIC	Home Affairs	DTA
Number of personnel who separated in 2015–16 with clearance still sponsored by entity	205	4	127	1415	1
Number of personnel who separated in 2016–17 with clearance still sponsored by entity	138	3	86	1919	19
<b>TOTAL</b>	<b>343</b>	<b>7</b>	<b>213</b>	<b>3334</b>	<b>20</b>

Source: ANAO analysis of entity personnel records and AGSVA clearance data.

3.66 Entities informed the ANAO that for some of these individuals, they had taken steps to inform AGSVA of their separation, but not those required by AGSVA and, as a result, their sponsorship had not been withdrawn.<sup>60</sup> However, in all cases, there were individuals sponsored by entities that should have had their sponsorship withdrawn. All entities were thus partially compliant with the PSPF mandatory control (associated with PERSEC-9) that: ‘Agencies **are to** advise the vetting agency of separation of personnel’.<sup>61</sup> This finding highlights weaknesses in entity assurance mechanisms relating to their clearance holder records.

3.67 While AGSVA has a role to play in ensuring that clearance holder records are accurate, entities have greater visibility as to which of their personnel are presently engaged and require a clearance. Entities implementing the quality assurance mechanisms outlined in Recommendation no.6 (paragraph 3.37) should help to address this issue.

60 For example, entities informed the ANAO that they had provided email advice to AGSVA that personnel had separated. However, sponsorship had not been withdrawn because AGSVA requires entities to log onto the Security Officer Dashboard and manually remove sponsorship of individuals.

61 AGD, *Personnel security guidelines—Agency personnel security responsibilities*, version 1.1, Canberra, April 2015, p. 48. Emphasis in original.

## Do entities effectively monitor and report on compliance with personnel security requirements?

All entities had reported their compliance with the PSPF personnel security requirements for 2016–17 to relevant parties. The ANAO's assessment of compliance differed from each entity's self-reported compliance level.

3.68 The PSPF requires entities to complete an annual security assessment to determine their compliance with the mandatory requirements of the PSPF, and to report any non-compliance to their relevant portfolio minister, AGD and the Auditor-General by 31 August each year (GOV-7).<sup>62</sup> The ANAO examined entity 2016–17 compliance reports and compared reported levels of compliance for PSPF personnel security requirements with the findings of this audit. The results of this analysis are at Table 3.12.

3.69 The ANAO employed the following assessment criteria:

- where entities met the mandatory requirement and all associated mandatory controls, they were rated as 'fully compliant';
- where entities were non-compliant with an associated mandatory control or the ANAO identified limited instances of non-compliance with mandatory requirements (indicating weaknesses in entity assurance mechanisms), they were rated as 'partially compliant'; and
- where entities had not implemented measures to comply with a mandatory requirement, they were rated as 'non-compliant'.<sup>63</sup>

3.70 All entities informed the ANAO that they have taken, or are planning to take, actions to address areas of partial compliance or non-compliance identified through this audit.

3.71 As part of its current reforms to the PSPF, AGD is planning to move away from a compliance reporting model and instead require entities to report on their protective security maturity, with the aim of shifting the reporting focus to security outcomes and providing a more nuanced approach to assessing security matters. In designing the new model, AGD should ensure that meeting mandatory requirements of the framework remains a core expectation. It should also consider developing assurance mechanisms that minimise entities' incentives to present an overly favourable interpretation of their maturity levels.



Grant Hehir  
Auditor-General

Canberra ACT  
11 May 2018

62 Agencies must also advise non-compliance to ASIO for matters relating to national security, the Australian Signals Directorate for matters relating to information security, and heads of any affected entities.

63 AGD requests that entities classify their PSPF compliance as either 'fully compliant', 'non-compliant' or 'not applicable'. It does not recognise a category of 'partial' compliance. The ANAO's assessment criteria were developed to provide a more granular assessment of compliance.

**Table 3.12: Entity self-reported<sup>a</sup> compliance ratings for personnel security and ANAO ratings of entity compliance, 2016–17**

PSPF requirement	Entity	Entity rating	ANAO rating
PERSEC-1 Conduct employment screening on personnel	AGD	●	●
	ARPANSA	●	●
	ASIC	●	●
	Home Affairs	●	●
	DTA	●	●
PERSEC-2 Establish ongoing suitability policies and procedures	AGD	●	●
	ARPANSA	●	●
	ASIC	●	●
	Home Affairs	●	●
	DTA	●	●
PERSEC-3 Identify, record and review positions requiring clearances	AGD	●	●
	ARPANSA	●	●
	ASIC	●	●
	Home Affairs	●	●
	DTA	●	●
PERSEC-4 Ensure personnel have appropriate clearances	AGD	●	●
	ARPANSA	●	●
	ASIC	●	●
	Home Affairs	●	●
	DTA	●	●
PERSEC-5 Follow eligibility waivers requirements	AGD	●	●
	ARPANSA	●	●
	ASIC	●	●
	Home Affairs	●	●
	DTA	●	●
PERSEC-6 Use AGSVA for clearances	AGD	●	●
	ARPANSA	●	●
	ASIC	●	●
	Home Affairs	●	●
	DTA	●	●
PERSEC-7 Establish clearance maintenance policies and procedures	AGD	●	●
	ARPANSA	●	●
	ASIC	●	●
	Home Affairs	●	●
	DTA	●	●
PERSEC-8 Share information relating to ongoing suitability	AGD	●	●
	ARPANSA	●	●
	ASIC	●	●
	Home Affairs	●	●
	DTA	●	●
PERSEC-9 Establish separation policies and procedures	AGD	●	●
	ARPANSA	●	●
	ASIC	●	●
	Home Affairs	●	●
	DTA	●	●

Key: ● Fully compliant    ● Partially compliant    ● Non-compliant

Note a: While in some cases entities reported 'partial' compliance, entity ratings in this table have been adjusted to conform to AGD's classification options.

Source: Entity PSPF compliance reporting to their portfolio ministers and ANAO analysis of entity compliance.

# Appendices

## Appendix 1 Entity responses

### Attorney-General's Department



**Australian Government**  
**Attorney-General's Department**  
**Secretary**

17/7376

21 March 2018

Ms Lisa Rauter  
Group Executive Director  
Performance Audit Services Group  
Australian National Audit Office  
GPO Box 707  
CANBERRA ACT 2601

Dear Ms Rauter

Thank you for the opportunity to comment on the proposed audit report on Mitigating Insider Threats through Personnel Security. I welcome the report and I am grateful for the recommendations made to better manage personnel security risks both across Australian Government, and within the Attorney-General's Department.

The timing of this report is helpful noting given the department is currently reforming the Protective Security Policy Framework (PSPF) for application from 1 July 2018. A revised PSPF will provide a clearer and more accessible framework, specify requirements that are proportional to risks, integrate more coherently with other frameworks, and improve the Commonwealth's approach to managing security risk. This report will continue to inform these reforms.

Please find below our response to the individual recommendations within the report:

**Recommendation No.1: Defence, in consultation with AGD, establish operational guidelines for, and make appropriate risk-based use of, clearance maintenance requirements.**

Agree. The department acknowledges the importance of the effective use of clearance maintenance requirements to allow entities to engage with and manage risks associated with their security cleared personnel's access to Australian Government resources. The department commits to providing Defence with information and support to enable AGSVA to make greater use of clearance maintenance requirements. The department will also use existing stakeholder forums to discuss and support the use of clearance maintenance. The department will continue to consult with Defence on the development of a framework to assess the ongoing suitability of security clearance holders, including operational guidelines for sponsoring agencies.

**Recommendation No.3: AGD and Defence establish a framework to facilitate AGSVA providing sponsoring entities with specific information on security concerns and mitigating factors identified through the vetting process.**

Agree. The department acknowledges the importance of communicating risk information to sponsoring entities and other vetting agencies as part of the initial process of security vetting and to support the ongoing assessment of personnel's suitability to hold a security clearance. Sharing security relevant information within an entity and between entities is essential to appropriately safeguard Australian government resources and can help prevent and detect a range of threats, including the trusted insider threat.

The department, in consultation with Defence and a number of other departments and agencies, is developing a range of resources to support risk information sharing such as clearance suitability risk factor guidelines and a fact sheet on information sharing to address misconceptions about perceived limitations to information sharing, as well as specific mechanisms such as templates and guidance to support Defence, and other vetting agencies, in sharing risk information with sponsoring entities.

**Recommendation No. 5: AGD conduct a personnel security risk assessment that considers whether changes are needed to their protective security practices.**

Agree. The department previously engaged an external Risk Assessment consultant prior to the announcement of the machinery of government changes in 2017. This was put on hold to be reinitiated after the machinery of government changes were completed as our expectation was that these changes would have a significant impact on our security risk profile. The department is currently working with the consultant on the new terms of reference for the personnel and physical risk assessment to align with the new organisational structure.

**Recommendation No. 7: AGD implement quality assurance mechanisms to reconcile their personnel records with AGSVA's clearance holder records, and commence clearance processes for any personnel who do not hold a required clearance.**

Agree. The department has recently concluded a full review of all its clearance holder records and can confirm that all staff either hold the required clearance or have commenced the security clearance process. We are in the process of transferring and/or cancelling sponsorship of clearances that should no longer be sponsored by the department. Going forward, the department will conduct an annual review of clearance holder records to ensure the accuracy of our records.

**Recommendation No. 8: AGD review their policies and procedures for eligibility waivers to ensure they are compliant with PSPF mandatory controls.**

Agree. The department has implemented an ICT solution where eligibility waivers are stored and information relating to the waiver is documented. This will ensure we can access the relevant information immediately and support the annual reassessment of all waivers, in accordance with PSPF requirements.

**Recommendation No. 9: AGD implement the PSPF requirement to undertake an annual health check for clearance holders and their managers.**

Agree. The department is developing options for a new process to implement a yearly health check including to align with the Program for Performance Improvement process which occurs 30 June every year.

Finally, I would like to thank your staff for the professional and collegiate manner in which this audit was conducted. We are committed to the implementation of the recommendations and continued improvement in this area.

The contact officer for this matter is Emma Appleton, Director, Governance Office who can be contacted on (02) 6141 2905

Yours sincerely



Chris Moraitis PSM



## Australian Radiation Protection and Nuclear Safety Authority



Australian Government  
 Australian Radiation Protection  
 and Nuclear Safety Agency



Ref: R18/03555

Lisa Rauter  
 Group Executive Director  
 Performance Audit Services Group  
 Australian National Audit Office

Dear Ms Rauter

**Re: Australian Radiation Protection and Nuclear Safety Agency Response to the ANAO Proposed Audit Report on Mitigating Insider Threats through Personnel Security**

I refer to your correspondence dated Tuesday 27 February 2018 where you sought comments from ARPANSA on the extract of the ANAO Proposed Audit Report on Mitigating Insider Threats through Personnel Security by Tuesday 27 March 2018.

As per your request, please consider this letter our formal letter of reply to be published in full as an appendix. Further, our summary response can be found at Attachment A and responses to recommendations at Attachment B.

ARPANSA welcomed the ANAO audit on our personnel security program and supporting systems. The audit provided a great opportunity for our agency to measure the effectiveness of one element of our protective security program, that being the personnel security component. Importantly, the audit highlighted that, for the most part, ARPANSA has an effective and robust program ensuring the appropriate level of protection for our people, information and assets. The audit identified areas where further efforts can be directed to ensure the agency is proactive in the way we manage eligibility and ongoing suitability of employees and contractors.

The audit findings reinforced the need for greater information sharing between ourselves and AGSVA, among others. As such ARPANSA will continue to develop systems and processes to allow for this and will look to establish additional relationships with relevant agencies and organisations across a range of protective security matters.

Further areas for improvement outlined throughout the report I consider to be quality management system (QMS) matters, specifically ensuring our employment screening consent forms are current as well as several documents not being updated within appropriate timeframes. While the requirements have always been a part of our QMS, we are committed to ensuring this is managed in a way that is considered best practice, noting we are close to implementing an integrated management system that has been two years in the design and development.

619 Lower Plenty Road, Yallambie VIC 3085  
 +61 3 9433 2211

38-40 Urunga Parade, Miranda NSW 2228  
 PO Box 655, Miranda NSW 1490  
 +61 2 9541 8333

info@arpansa.gov.au  
 arpansa.gov.au

In response to the two recommendations for ARPANSA I provide the following:

**Recommendation No. 8:** ARPANSA review their policies and procedures for eligibility waivers to ensure they are compliant with PSPF mandatory controls.

**Response:** ARPANSA agrees with this recommendation. ARPANSA has updated our policy and procedures to reflect the requirement to undertake risk assessments every year for those who have been granted an eligibility waiver.


**Recommendation No. 9:** ARPANSA implement the PSPF requirement to undertake an annual health check for clearance holders and their managers.

**Response:** ARPANSA agrees with this recommendation. Following the security risk assessment conducted in June 2017 by the Agency Security Group, the annual health check was firmly placed in the 2017/18 FY program of works. Consultation and coordination efforts with ARPANSA's People and Culture has occurred since that time to design and implement the health checks in a manner that is consistent with the agency's people management program. The health checks are expected to roll out within the 2018 calendar year.

To conclude, the audit provided two recommendations that I am comfortable with as well as several non-mandatory areas for improvement that verified our recent compliance reporting advice to our Minister. This has provided me with a high degree of confidence in our assessment of the effectiveness of our protective security program.

I would like to take this opportunity again to thank the ANAO for the professional conduct in which the audit was carried out.

Regards



**Carl-Magnus Larsson**  
CEO ARPANSA

26 March 2018

## Australian Securities and Investments Commission



**JAMES R F SHIPTON**  
Chair

Level 7, 120 Collins Street, Melbourne  
GPO Box 9827 Melbourne VIC 3001

Direct: +61 3 9280 4100 - Melbourne  
Email: [james.shipton@asic.gov.au](mailto:james.shipton@asic.gov.au)  
Web: [www.asic.gov.au](http://www.asic.gov.au)

29 March 2018

Ms Lisa Rauter  
Group Executive Director  
Performance Audit Service Group  
AUSTRALIAN NATIONAL AUDIT OFFICE

By email: <[Lisa.Rauter@anao.gov.au](mailto:Lisa.Rauter@anao.gov.au)>

### ASIC REPLY TO ANAO AUDIT REPORT ON MITIGATING INSIDER THREATS THROUGH PERSONNEL SECURITY

Dear Ms Rauter,

I refer to your email dated 1 March 2018, enclosing the extract of a proposed audit report on *Mitigating Insider Threats through Personnel Security*, prepared by the Australian National Audit Office (ANAO).

ASIC concurs with the three recommendations applicable to ASIC in the report.

Attached is a short summary of ASIC's responses for inclusion in the Summary section of the final report (**Attachment A**); and ASIC's formal response to the recommendations for inclusion in the final report (**Attachment B**).

Also, attached are ASIC's editorial comments as requested in your email (**Attachment C**).

Yours sincerely,

James R. F. Shipton  
Chair

Encl.

# Australian Security Intelligence Organisation



**Australian Government**

**Australian Security  
Intelligence Organisation**

**Director-General of Security**

28 March 2018  
Ref: A14755746

Mr Grant Hehir  
Auditor-General  
Australian National Audit Office  
19 National Circuit  
Barton ACT 2601

*Dear Mr Hehir,*

I would like to acknowledge the Australian National Audit Office (ANAO) performance audit on *Mitigating Insider Threats through Personnel Security*, and for the opportunity to comment on the Section 19, proposed report provided to ASIO on 27 February 2018.

The Australian Government Security Vetting Agency (AGSVA) is responsible for the majority of Australian Government clearances issued annually. As such, AGSVA's vetting decisions have a real and direct impact on the security of Australian Government personnel, information and resources.

ASIO plays a key role in the security clearance process. We contribute our national security expertise to assess clearance applicants at the Negative Vetting 1 (NV1), NV2 and Top Secret Positive Vetting (PV) levels. In formulating our security assessments, ASIO considers information provided by the vetting agency in the context of ASIO's information holdings and our unique understanding of the threat environment.

ASIO security assessments provide a recommendation to the vetting agency on the suitability of the clearance subject to access national security classified information and resources. ASIO's assessment is not a recommendation to grant or deny a clearance; consistent with the Personnel Security Guidelines, that remains the vetting agency's responsibility. ASIO is not positioned to conduct whole-of-government vetting, nor do our assessments constitute quality control or validation of the vetting agencies' decisions. ASIO's security assessment is an important national security layer in the clearance process but is only one aspect of the process.

GPO Box 2176  
Canberra City ACT 2601  
Telephone: 02 6249 6299  
Facsimile: 02 6257 4501

**FOI WARNING:**  
Exempt document under  
*Freedom of Information Act 1982.*  
Refer related FOI requests to  
Attorney-General's Department, Canberra.

In this, ASIO is a key partner in AGSVA's vetting work and we support a strong and effective AGSVA. I acknowledge there are ongoing challenges in meeting the increasing demand for clearances, particularly at the PV level. ASIO continues to work in close partnership with AGSVA to address concerns identified in the ANAO Audit, including improving quality of vetting outcomes and clearance processing times.

ASIO is consistently responding to requests for personnel security assessments for NV1 and NV2 security clearances well within timeframes agreed with AGSVA. As reported in ASIO's 2016-17 annual report, we are not responding within agreed timeframes for PV clearances – the most resource-intensive clearances – due to a significant increase in demand. It is unlikely the agreed timeframes will be met for this class of security clearances by the end of 2017–18. However, ASIO responds to the majority of priority PV requests within agreed timeframes.

ASIO also continues to work closely with AGSVA on PV clearances and has implemented a range of initiatives to improve response times. As a result, over the last six months, ASIO is generally matching AGSVA's referral rate, and in 2018 has finalised more assessments than referrals received, resulting in an overall reduction of outstanding case numbers. We expect this to continue for the remainder of 2017-18, though resourcing fluctuations will continue to influence finalisation rates.

ASIO also contributes to broader initiatives to improve vetting outcomes.

- In accordance with the recommendations of the 2017 Independent Intelligence Review, ASIO is commencing secondments of ASIO staff to AGSVA, which will build upon our existing cooperation through improved mutual understanding and contribute to improving security outcomes for government.
- ASIO is a supporting AGSVA's ICT2270 Vetting Transformation project as a key stakeholder.
- We are contributing to the Attorney General's Department (AGD)-led review of the Personnel Security Protective Framework policy, which aims to enhance vetting outcomes including through improved information sharing between vetting and sponsor agencies.

ASIO's security expertise is a vital component of the security clearance process and adds independent value to the vetting process. We are committed to continuing our close partnership with AGSVA to allow for ongoing improvement to the quality and responsiveness of vetting outcomes for better risk management of Australian Government personnel, information and resources.

*Yours sincerely,  
Duncan Lewis*

Duncan Lewis

GPO Box 2176  
Canberra City ACT 2601  
Telephone: 02 8249 6299  
Facsimile: 02 8257 4501

**FOI WARNING:**  
Exempt document under  
Freedom of Information Act 1982.  
Refer related FOI requests to  
Attorney-General's Department, Canberra.



**Australian Government**  
**Department of Defence**

**Ms Rebecca Skinner**  
**Acting Secretary**

**Air Chief Marshal MD Binskin, AC**  
**Chief of the Defence Force**

SEC/OUT/2018/87  
CDF/OUT/2018/282

**Mr Grant Hehir**  
Auditor-General  
PO Box 707  
CANBERRA ACT 2601

Dear Hehir,

**DEFENCE RESPONSE - ANAO SECTION 19 PROPOSED REPORT – MITIGATING  
INSIDER THREATS THROUGH PERSONNEL SECURITY**

Thank you for your correspondence of 27 February 2018, which contained the Section 19 Proposed Report – *Mitigating Insider Threats through Personnel Security*.

Defence appreciates the opportunity to review and comment on the report and notes the reform efforts already underway to mitigate the malicious insider threat. The Report draws attention to personnel security reform efforts already in development, led by the Attorney General's Department, in close consultation with Defence. Additionally, Defence notes that the Report highlights the internal reform efforts the Australian Government Vetting Agency (AGSVA) have undertaken and the improvement in AGSVA's performance over the last two years. AGSVA is still undertaking a significant reform program with many of the issues flagged in the Report being addressed through reform implementation in the next year.

The Report highlights mechanisms for information sharing that will guide agencies to develop clearance maintenance requirements. These are being actively considered and developed by the Attorney General's Department, as the Commonwealth protective security policy lead, in conjunction with AGSVA as the main service delivery agency for security vetting.

It should be noted that Defence is implementing a program to improve security controls within the existing eVetting System, ahead of the delivery of the new system being implemented. AGSVA is working with cross-government and industry partners to ensure that the eVetting System and the systems with which it interfaces meet contemporary security standards.

**PO Box 7900, Canberra BC, ACT 2610**  
**[www.defence.gov.au](http://www.defence.gov.au)**

*Defending Australia and its National Interests*

Attached to this letter are Defence's Proposed Amendments, Editorials and Comments (**Annex A**), Response to Recommendations (**Annex B**) and the Agency Response (**Annex C**). These constitute Defence's formal response to the Section 19 Proposed Report.

As set out in Annex B, Defence agrees with all of the proposed recommendations for this audit.

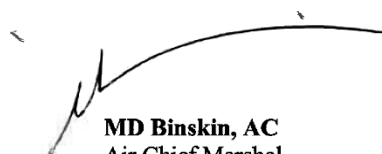
Defence remains committed to assisting you with the successful completion of this audit. We look forward to the upcoming Final Report.

Yours sincerely,



**Rebecca Skinner**  
Acting Secretary

16 April 2018



**MD Binskin, AC**  
Air Chief Marshal  
Chief of the Defence Force

17 April 2018

**Annexes**

- A. Defence's Proposed Amendments, Comments, and Editorials
- B. Defence's Response to Recommendations
- C. Defence's Agency Response

## Department of Home Affairs



**Australian Government**  
**Department of Home Affairs**

---

Lisa Rauter  
Group Executive Director  
Performance Audit Services  
Australian National Audit Office  
GPO Box 707  
Canberra ACT 2601

Dear Ms Rauter,

Thank you for the opportunity to provide comments on the ANAO's audit report on *Mitigating Insider Threats through Personnel Security*.

The Department of Home Affairs responds on the basis that the redactions noted in the report are not relevant to the Department. The report's recommendations appear to be an accurate reflection regarding areas for improvement in Home Affairs.


The Department provides comments at Attachment A regarding Recommendations 7 and 9, and also two comments at Attachment B which clarify a footnote and request an update to data in Table 3.1 of the report.

Thank you for your conduct of this Audit and I am pleased that we were able to assist your office through the process of the Audit.

If you would like to further discuss our response to the Report, please contact Mr David Norris (Assistant Secretary, Audit and Assurance) on [david.norris@homeaffairs.gov.au](mailto:david.norris@homeaffairs.gov.au) or (02) 6264 2022.

Yours sincerely

(Electronically signed)

  
**Cheryl-anne Moy**  
Chief Audit Executive  
First Assistant Secretary  
Integrity, Security and Assurance Division

27 March 2018

---

6 Chan Street Belconnen ACT 2617  
PO Box 25 Belconnen ACT 2616 • Telephone: 02 6264 1111 • Fax: 02 6225 6970 • [www.homeaffairs.gov.au](http://www.homeaffairs.gov.au)



## Digital Transformation Agency



Australian Government  
Digital Transformation Agency

**dta**

PO Box 457  
CANBERRA ACT 2601  
[dta.gov.au](http://dta.gov.au)

March 2018

Ms Lisa Rauter  
Group Executive Director  
Performance Audit Services  
Australian National Audit Office  
GPO Box 707  
CANBERRA ACT 2601

Dear Ms Rauter

Thank you for providing the opportunity to comment on the Australian National Audit Office's (ANAO) proposed report on Mitigating Insider Threats through Personnel Security.

The Digital Transformation Agency (DTA) agrees with the ANAO's five recommendations and will ensure that all of the recommendations are implemented by 31 July 2018.

The DTA's response to the ANAO's proposed report including each of the relevant recommendations is outlined at Attachment A to this letter.

If you would like to discuss the DTA's response further, please contact Mr George-Philip de Wet, Chief Finance Officer by email at [george-philip.dewet@dta.gov.au](mailto:george-philip.dewet@dta.gov.au) or phone 0408 768 407.

Yours sincerely

A handwritten signature in black ink, appearing to read 'G Slater'.

Gavin Slater  
Chief Executive Officer

## Appendix 2 PSPF requirements related to personnel security

Reference	PSPF mandatory requirement
<b>Personnel security (PERSEC) requirements</b>	
PERSEC-1	Agencies must ensure that their personnel who access Australian Government resources (people, information and assets): <ul style="list-style-type: none"> <li>• are eligible to have access</li> <li>• have had their identity established</li> <li>• are suitable to have access</li> <li>• agree to comply with the Government's policies, standards, protocols and guidelines that safeguard the agency's resources from harm.</li> </ul>
PERSEC-2	Agencies must have policies and procedures to assess and manage the ongoing suitability for employment of their personnel.
PERSEC-3	Agencies must identify, record and review positions that require a security clearance and the level of clearance required.
PERSEC-4	Agencies must ensure their personnel with ongoing access to Australian Government security classified resources hold a security clearance at the appropriate level, sponsored by an Australian Government agency.
PERSEC-5	Before issuing an eligibility waiver (citizenship or checkable background) and prior to requesting an Australian Government security clearance an agency must: <ul style="list-style-type: none"> <li>• justify an exceptional business requirement</li> <li>• conduct and document a risk assessment</li> <li>• define the period covered by the waiver (which cannot be open-ended)</li> <li>• gain agreement from the clearance applicant to meet the conditions of the waiver</li> <li>• consult with the vetting agency.</li> </ul>
PERSEC-6	Agencies, other than authorised vetting agencies, must use [AGSVA] to conduct initial vetting and reviews.
PERSEC-7	Agencies must establish, implement and maintain security clearance policies and procedures for clearance maintenance in their agencies.
PERSEC-8	Agencies and vetting agencies must share information that may impact on an individual's ongoing suitability to hold an Australian Government security clearance.
PERSEC-9	Agencies must have separation policies and procedures for departing clearance holders, which includes a requirement to: <ul style="list-style-type: none"> <li>• inform vetting agencies when a clearance holder leaves agency employment or contract engagement</li> <li>• advise vetting agencies of any security concerns.</li> </ul>
<b>Governance (GOV) requirements relevant to personnel security</b>	
GOV-1	Agencies must provide all staff, including contractors, with sufficient information and security awareness training to ensure they are aware and meet the requirements of the [PSPF].
GOV-4	Agencies must prepare a security plan to manage their security risks. The security plan must be updated or revised every two years or sooner where changes in risks and the agency's operating environment dictate.

Reference	PSPF mandatory requirement
GOV-5	Agencies must develop their own set of protective security policies and procedures to meet their specific business needs.
GOV-6	Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the Australian Standards AS/NZS ISO 31000:2009 <i>Risk management—Principles and guidelines</i> and <i>HB 167: 2006 Security risk management</i> .
GOV-7	For internal audit and reporting, agencies must: <ul style="list-style-type: none"> <li>• undertake an annual security assessment against the mandatory requirements detailed within the [PSPF]</li> <li>• report their compliance with the mandatory requirements to the relevant portfolio Minister.</li> </ul>

Source: AGD, 'Mandatory requirements', PSPF web page, available from: <<https://www.protectivesecurity.gov.au/overarching-guidance/Pages/Mandatory-requirements.aspx>> [accessed 10 August 2017].

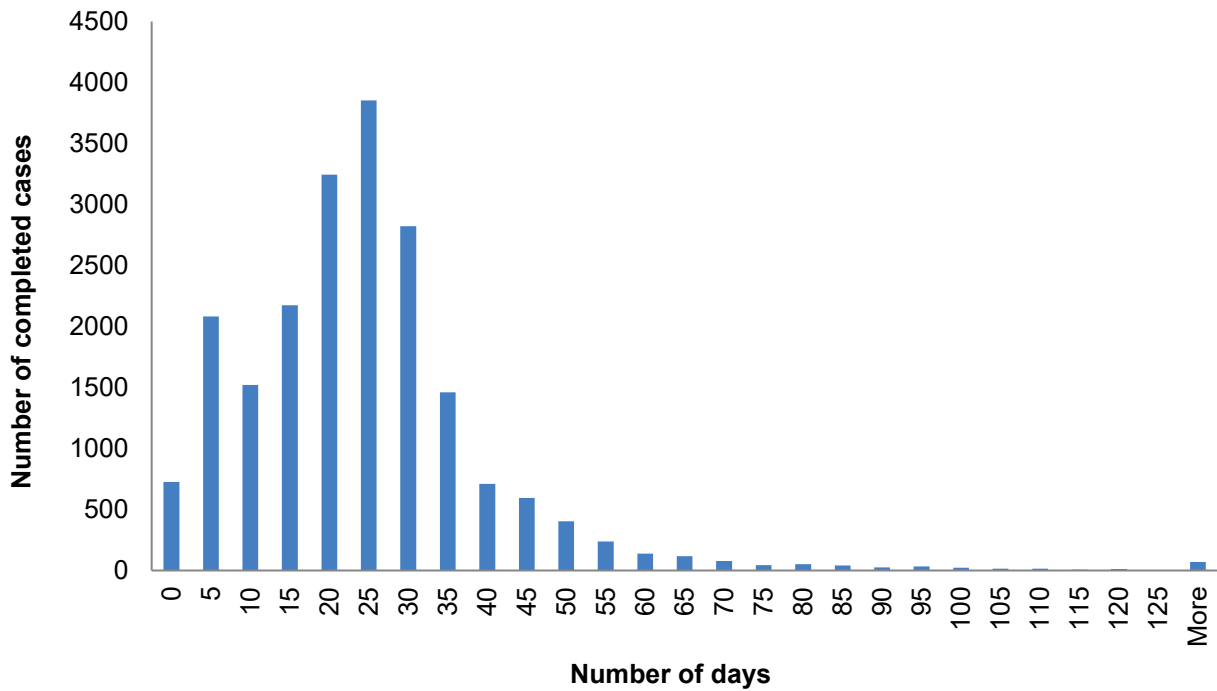
## Appendix 3 Minimum personnel security checks and requirements for initial clearances

			<b>Positive Vetting</b>
			Psychological assessment
		<b>Negative Vetting 2</b>	Financial probity check
	<b>Negative Vetting 1</b>	Security interview	Security interview
	Digital footprint checks	Digital footprint checks	Digital footprint checks
	Financial statement	Financial statement	Financial statement
	Suitability screening questionnaire	Suitability screening questionnaire	Suitability screening questionnaire
<b>Baseline Vetting</b>	ASIO assessment	ASIO assessment	ASIO assessment
Qualification verification	Qualification verification	Qualification verification	Qualification verification
Professional referee check	Referee checks (including 1 professional)	Referee checks (including 1 professional and 1 un-nominated)	Referee checks (including 1 professional and 1 un-nominated)
Police Records Check (No Exclusion)	Police Records Check (Full Exclusion)	Police Records Check (Full Exclusion)	Police Records Check (Full Exclusion)
Financial History Check	Financial History Check	Financial History Check	Financial History Check
5 year background check	10 year background check	10 year background check	10 year background check or from 16 years of age, whichever is greater
Official secrets declaration	Official secrets declaration	Official secrets declaration	Official secrets declaration
Statutory declaration	Statutory declaration	Statutory declaration	Statutory declaration
Identity verification	Identity verification	Identity verification	Identity verification

Source: AGD, *Personnel security guidelines—vetting practices*, version 1.3, June 2016, p. 20.

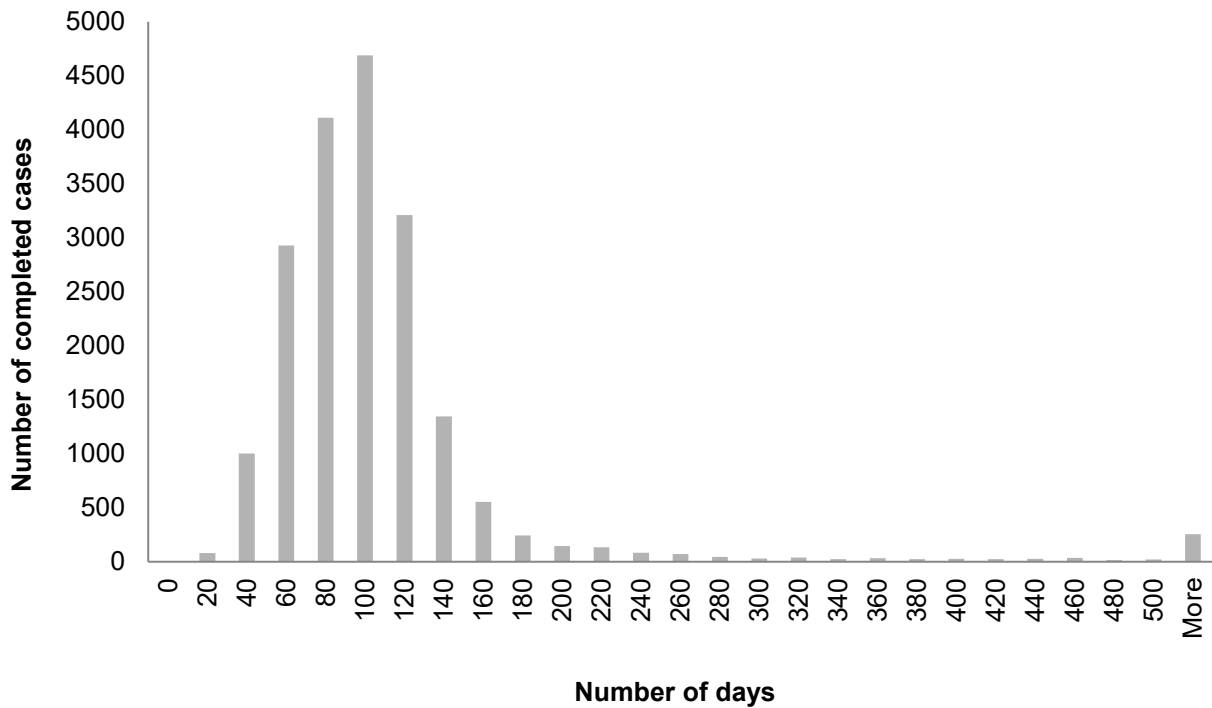
## Appendix 4 AGSVA's clearance timeframes

**Figure A.1: Distribution of Baseline clearance timeframes, 2016–17**



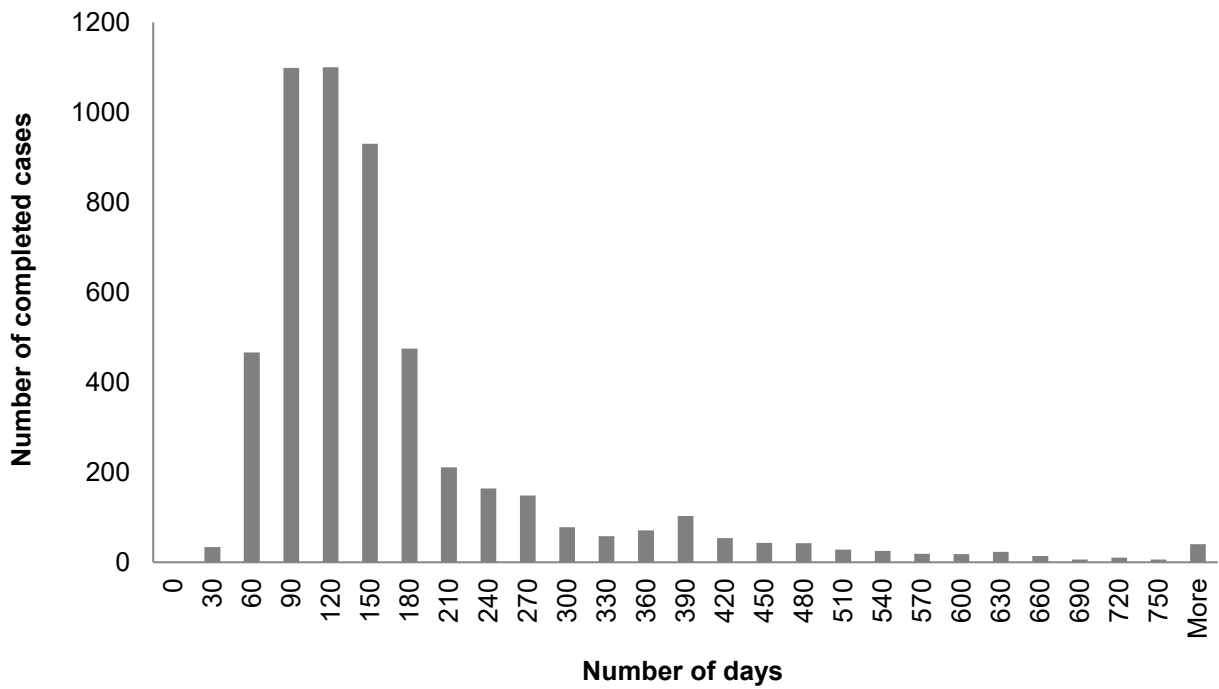
Source: ANAO analysis of AGSVA clearance data.

**Figure A.2: Distribution of NV1 clearance timeframes, 2016–17**



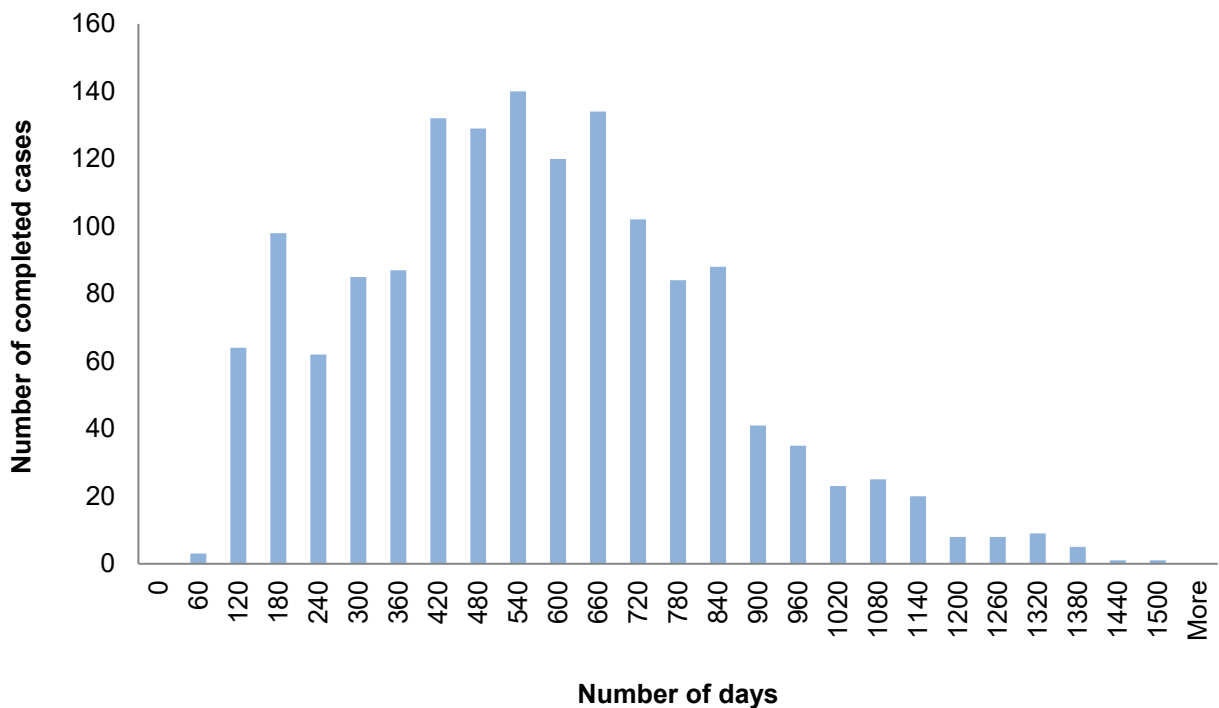
Source: ANAO analysis of AGSVA clearance data.

**Figure A.3: Distribution of NV2 clearance timeframes, 2016–17**



Source: ANAO analysis of AGSVA clearance data.

**Figure A.4: Distribution of PV clearance timeframes, 2016–17**



Source: ANAO analysis of AGSVA clearance data.

## Appendix 5 Assessment criteria for personnel security governance

1. For the qualitative assessment in Table 3.1 of the report, entities were assessed against the criteria and considerations outlined in Table A.1. These criteria and considerations were developed based on mandatory controls (in **bold** in Table A.1) and recommended actions outlined in PSPF policy documents, with a focus on governance components of the PSPF that intersect with personnel security.

**Table A.1: Criteria and considerations for assessing entity security plans, policies, procedures and risk assessments**

Criterion	Consideration <sup>a</sup>
Has the entity undertaken regular security planning with adequate oversight and consultation?	<b>Has the entity developed a protective security plan to manage its security risks?</b>
	<b>Has the plan been reviewed at least every two years or sooner if the risk or operating environment has changed?</b>
	<b>Was the plan developed based on a security risk assessment?</b>
	Has the plan been endorsed by the accountable authority or a delegate?
	Was the security plan developed through consultation with relevant staff and with senior management input and support?
Does the entity's security plan adequately cover personnel security?	Does the plan adequately cover personnel security measures and actions (e.g. provisions in recruitment process, positions requiring clearances, contact reporting, aftercare, awareness training)?
	Are personnel security measures and actions informed by a personnel security risk assessment?
	Do personnel security components of the plan follow the suggested format (e.g. assessment of existing measures; actions/strategies, resources and responsibilities and outcomes/KPIs)?
Are the entity's policies and procedures current, accessible and subject to adequate oversight and review?	<b>Has the entity developed protective security policies and procedures to meet its specific business needs?</b>
	<b>Have the policies and procedures been reviewed at least every two years?</b>
	<b>Was the policy developed based on a security risk assessment?</b>
	Has the policy been endorsed by the accountable authority or a delegate?
	Are the policies and procedures easily accessible by all employees?
Do the policies and procedures adequately cover personnel security?	<b>Has the entity developed policies and procedures to monitor ongoing suitability of staff, based on its risk assessment?</b>
	Does the policy adequately cover personnel security policy (e.g. agency specific checks, clearance requirements, temporary access)?
	Has the entity developed any procedures to inform employees of personnel security requirements?
Has the entity recently undertaken a security risk assessment?	<b>Has the entity undertaken a security risk assessment to identify, evaluate and treat risks to its critical assets?</b>
	Was the latest assessment undertaken within the last two years?

Criterion	Consideration <sup>a</sup>
Has the entity adequately considered personnel security risks as part of its security risk management process?	<b>Has the entity used the risk assessment to determine what checks are required for personnel security?</b>
	Has the entity undertaken a personnel security risk assessment and/or considered personnel security risks as part of its security risk management process?

Note a: Considerations in bold print are mandatory controls.

Source: ANAO.



## Appendix 6 Methodology for matching AGSVA clearance holder data and entity personnel data

1. Entities and AGSVA do not consistently use a common identifier that could be used to match entity staff with their AGSVA clearance file. AGSVA makes use of a Clearance Subject Identifier (CSID), which is not consistently recorded by entities. Entities typically use AGS numbers to identify staff (which is not consistently recorded by AGSVA) and other identifiers for external personnel (such as contractors).
2. In order to determine the extent to which entity personnel held clearances with AGSVA, the ANAO developed a methodology to reconcile entities personnel records with AGSVA's clearance records, using the basic biographical data shared between the two. Due to data inconsistencies, potential matches are assigned a confidence on the basis shown in Table A.2 below.

**Table A.2: ANAO methodology for matching entity staff to AGSVA clearances**

Clearance holder attributes	Confidence of ANAO match to AGSVA clearance
First name, last name, full date of birth	High
First initial, last name, full date of birth	High
Last name, full date of birth	Medium
First name, full date of birth	Medium
First initial, last name, day of birth, month of birth	Low
First initial, last name, year of birth	Low

Source: ANAO.

