The Auditor-General
ANAO Report No.45 2014–15
Performance Audit

Central Administration of Security Vetting

Department of Defence

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76033-056-9 (Print)
ISBN 978-1-76033-057-6 (Online)

Office of the Auditor-General for Australia

Australian National Audit Office

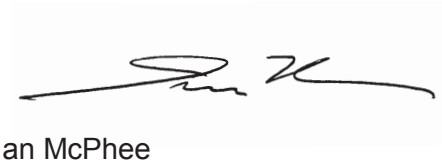
Canberra ACT
9 June 2015

Dear Mr President
Dear Madam Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Department of Defence titled *Central Administration of Security Vetting.* 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



Ian McPhee

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:

The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7505
Fax: (02) 6203 7519
Email: publications@anao.gov.au

ANAO audit reports and information about the ANAO are available on our website:

http://www.anao.gov.au

Audit Team

Jennifer Myles
Jed Andrews
Stuart Turnbull

Contents

Tables

Figures

Abbreviations

AGD	Attorney-General's Department
AGSVA	Australian Government Security Vetting Agency
AO	Assessing Officer
ANAO	Australian National Audit Office
ASVS	Australian Security Vetting Service
ASIO	Australian Security Intelligence Organisation
DSA	Defence Security Authority
IGIS	Inspector-General of Intelligence and Security
IVP	Industry Vetting Panel
NV	Negative Vetting
PSAMS	Personnel Security Assessment Management System
PSF	Personal Security File
PSPF	Protective Security Policy Framework
PV	Positive Vetting
SCNS	Secretaries' Committee on National Security

Glossary

Assessing Officer	A qualified person who conducts personnel security clearance assessments in accordance with the procedures outlined in the Protective Security Policy Framework (PSPF).
Authorised vetting agency	A Commonwealth entity authorised to undertake security vetting and grant security clearances to meet entity business needs.
Clearance holder	An individual who currently holds a security clearance.
Clearance subject	An individual whose suitability to hold a security clearance is being assessed by AGSVA.
Delegate	An officer appointed by Defence's Chief Security Officer to make the final decision regarding a clearance subject's suitability to hold a security clearance.
Need-to-know	Refers to a need to access information based on an operational requirement. Access to official information should be limited to those who require access to do their work.
Ongoing clearance maintenance	The ongoing personnel security management framework including the periodic review of all clearances.
Personnel security	The management of personnel to assist in the protection of an entity's people, information and assets. This includes initial and ongoing screening, and ongoing education and evaluation of personnel. One aspect of personnel security is the security vetting process.
Protective security	A combination of procedural, physical, personnel, and information security measures designed to protect people, information and assets from security threats.

Re-evaluation	Refers to the revalidation of Positive Vetting level clearances.
Revalidation	The process of reviewing a previously cleared individual and making a reassessment about their continued suitability for the clearance by assessing any relevant change of circumstances and determining whether any security concerns have arisen. The term revalidation applies to all security clearance levels.
Security clearance	A documented determination by an authorised vetting agency that an employee is suitable to access security classified information (on a need-to-know basis) relative to the level of clearance granted.
Security vetting	Checking and assessment action to develop a realistic and informed evaluation of an individual's suitability to hold a security clearance.

Summary and Recommendations

Summary

Introduction

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

2. Australian Government entities managed their own security vetting for employees and contractors until the end of September 2010. The Australian Government Security Vetting Agency (AGSVA) was then established within the Department of Defence (Defence) from 1 October 2010 to centrally administer personnel security vetting on behalf of Australian Government entities.[1] 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 security vetting service; and cost savings of $5.3 million per year.

3. Most government entities must use AGSVA's security vetting service for personnel that require a clearance.[2] AGSVA's vetting process involves enquiry into, and corroboration of, a person's background, character and personal values, before a decision is made by AGSVA on whether to grant or continue a clearance. AGSVA has management responsibilities for some 349 000 active Australian Government security clearances, and issued over 33 000 clearances in 2013–14.

1 Before the establishment of AGSVA, over 100 government entities were responsible for managing their own security vetting processes, and over 50 of those entities held separate contracts with vetting service providers.

2 Other authorised vetting agencies include the Australian Federal Police (AFP), the Department of Foreign Affairs and Trade (DFAT) and those Australian Intelligence Community agencies not in the Department of Defence. These agencies are responsible for conducting their own security vetting.

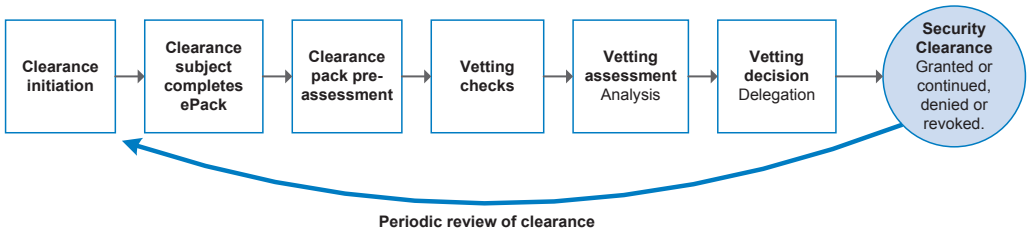
Australian Government Security Vetting Agency (AGSVA)

4. AGSVA forms part of Defence's Intelligence and Security Group. The agency includes: an executive group in Canberra; a National Coordination Centre in Brisbane; a Vetting Support Centre in Adelaide; and regional offices in each state and territory, which manage security vetting assessments and determinations. As at 30 March 2015, AGSVA employed 272 Australian Public Service (APS) staff, including some 130 Assessing Officers (AOs). AGSVA also manages a contracted workforce of over 300 personnel, who provide administrative support, and conduct vetting and psychological assessments. AGSVA's Industry Vetting Panel (IVP) comprises 21 companies and approximately 200 AOs, who complete around half of AGSVA's vetting assessments.

5. Figure S.1 illustrates AGSVA's security vetting process. Each individual subject to the vetting process provides mandatory information using AGSVA's ePack system, and sends AGSVA supporting documentation. AGSVA then assesses the submitted information for completeness, and initiates or conducts a range of vetting checks, such as referee checks, a police records check and a financial history check. An AO analyses the information provided by the individual and the results of checks undertaken, and requests further information and conducts interviews as necessary. The AO then makes a recommendation on the suitability of the individual to hold a clearance at the requested level to an AGSVA Delegate, who reviews the case and makes a decision. AGSVA charges government entities (other than Defence) on a fee-for-service basis for each clearance request.[3]

3 While funding for Defence personnel security clearances is included within Defence's budget, Defence does not notionally charge Defence Groups and Services for the cost of these clearances. As of 1 January 2015, Defence commenced charging Defence industry for the cost of security vetting services provided for Defence contractors.

Figure S.1: Overview of the security vetting process



Source: ANAO analysis of AGSVA documentation and processes.

Personnel security policy and clearance levels

6. A decision about granting a security clearance should be made in accordance with the standards identified in the Australian Government Protective Security Policy Framework (PSPF).[4] Vetting assessments and decisions are to take into account all available and reliable information, whether favourable or unfavourable, about the clearance subject. The Personnel Security Core Policy states that: 'Any doubt about the suitability of a clearance subject is to be resolved in favour of the national interest.'[5]

7. The PSPF identifies four levels of security clearance: Baseline, Negative Vetting 1 (NV1), Negative Vetting 2 (NV2) and Positive Vetting (PV). Higher level clearances involve additional vetting checks and allow personnel to access increasing levels of classified resources. Under the PSPF, AGSVA is responsible for initiating periodic reviews of security clearances at set intervals, ranging from 15 years for Baseline to five years for PV clearances.

8. In late 2014, the Attorney-General's Department (AGD) introduced a number of reforms to personnel security policy. The reforms are intended to clarify the responsibilities of government entities, direct resources to the areas of greatest risk and further strengthen the assessment of a person's ongoing suitability to hold a security clearance. The reforms were initiated in response

4 The PSPF is managed by the Attorney-General's Department (AGD) and establishes controls for the Australian Government to protect its people, information and assets, at home and overseas. The PSPF includes the Personnel Security Core Policy, Personnel Security Protocol, Agency Personnel Security Responsibilities Guidelines and Vetting Practices Guidelines, which provide detailed policy and guidance on personnel security and security vetting.

5 AGD, *Australian Government Personnel Security Core Policy* [Internet], available from <http://www.protectivesecurity.gov.au/personnelsecurity/Pages/default.aspx> [accessed 24 September 2014].

to high profile international security incidents[6], which highlighted the potential consequences of inadequate security vetting and employer monitoring and reporting.

Audit objectives and scope

9. The audit objective was to examine whether the Department of Defence (Defence) provides an efficient and effective security vetting service for Australian Government entities through the Australian Government Security Vetting Agency (AGSVA).

10. The high-level criteria used to assess AGSVA's performance were:

- AGSVA's establishment was well planned and supported by an implementation strategy that enabled the agency to undertake the responsibilities conferred upon it;
- AGSVA has adequate guidelines, procedures and systems in place to support the security clearance process;
- AGSVA's security clearance policies and procedures comply with Australian Government policy, including the Protective Security Policy Framework (PSPF);
- AGSVA identifies areas for improvement in security clearance arrangements and implements strategies to enhance performance; and
- Defence monitors, evaluates and reports on the efficiency and effectiveness of AGSVA's security vetting service.[7]

6 For example, in 2013, Aaron Alexis killed twelve people and injured several others when he entered a United States (US) Navy facility with a shotgun using a security clearance which had been issued in 2008. Investigations by the US House of Representatives have found that the background check which led to the issue of the clearance failed to detect his prior history of firearms offences, and that instances of erratic behaviour after the clearance was issued had not been reported. The company which conducted Alexis' background checks was also found to have conducted the checks for Edward Snowden, who was issued with a Top Secret clearance and has since been accused of unauthorised disclosure of classified information. In January 2014, the US Justice Department filed a complaint against the company, US Investigation Services (USIS), for providing incomplete background investigations between March 2008 and September 2012.

7 The audit did not assess whether individual security clearances have been appropriately granted or denied.

Overall conclusion

11. Security vetting involves the assessment of an individual's suitability to hold a security clearance at a particular level. Australian Government employees and contractors require a security clearance to access classified resources, which can relate to Australia's national security, economic and other interests; and security vetting of individuals in positions of trust is an important risk mitigation activity for the protection of such government resources.

12. In November 2009, the then Government decided to establish AGSVA within Defence to perform security vetting for most Australian Government entities on a fee-for-service basis, replacing a decentralised system in which individual entities managed personnel security vetting based on Australian Government policy requirements. The Government expected that centralised vetting would: result in a more efficient vetting process; improve the consistency of vetting practices; and deliver $5.3 million in annual cost savings.

13. Overall, the performance of the centralised vetting system established in October 2010 has been mixed, and key Australian Government expectations relating to improved efficiency and cost savings have not been realised. AGSVA was not ready to effectively provide whole-of-government vetting services in 2010 due to inadequate implementation planning, risk management and resourcing. While Defence has made progress since 2012 in its implementation of centralised vetting—by strengthening the management of vetting work, documenting its vetting procedures and applying additional human resources—AGSVA continues to fall well short of fully meeting its vetting responsibilities in a timely manner, and anticipated savings have been eroded. There is scope for Defence to develop a clear pathway to strengthen AGSVA's capacity to deliver services, and improve quality control over aspects of vetting practice and decision-making.

14. The mixed performance of centralised vetting has its roots in an inadequate policy proposal developed in 2009 by AGD in consultation with Defence and the then Department of Finance and Deregulation, which did not effectively assess Defence's capacity to deliver whole-of-government services with the resources proposed. AGSVA commenced operations on the back foot, with significantly reduced vetting resources compared to those previously deployed across government, and without an appropriate management structure, documented procedures and adequate ICT systems. The failure to identify and address key risks during the policy development and

implementation planning phases has had lasting consequences for AGSVA's delivery of vetting services.[8]

15. Over time, Defence has attempted to overcome identified shortcomings and improve AGSVA's performance. AGSVA's APS staffing level has been increased, as has utilisation of contractors to conduct security clearance assessments. These additional resources have been provided to AGSVA from within Defence's overall budget, eroding the savings originally anticipated from centralised vetting. Other key changes included: the introduction from 2012 of a revised management structure incorporating more appropriate governance arrangements; implementation of a centrally managed suite of procedural documentation; and the accreditation of AGSVA's Quality Management System to an internationally recognised standard in April 2014.[9] Notwithstanding these changes, AGSVA still needs to improve the level of assurance over IVP contractors' work practices through a targeted audit program, and strengthen quality control over vetting decisions through a review process. These measures would help address inconsistencies in vetting assessment processes identified by AGSVA, and concerns raised by some stakeholders about the rigour of AGSVA's assessment process.

16. Defence has invested over $37 million since 2008 in upgrading AGSVA's core ICT systems—ePack and the Personnel Security Assessment Management System (PSAMS)—expecting that the upgrades would make a marked difference to vetting performance. While the upgraded systems help ensure the completion of mandatory vetting tasks and compliance with policy requirements, they still lack reliability and functionality. The ePack system remains a frustrating and difficult system for individual users to navigate, raising efficiency and productivity issues in the vetting process. Further, there is at times a reliance on inefficient hard copy documentation processes. PSAMS also does not support certain tasks performed by AGSVA as part of the ongoing management of clearances. Notwithstanding Defence's substantial

8 The ANAO's *Successful Implementation of Policy Initiatives Better Practice Guide* identifies the importance of briefing the Government about key implementation risks and proposed responses, and that risks which suggest agreed timelines and resourcing are inadequate should be brought to the Government's attention.

Australian Government, Department of the Prime Minister and Cabinet and Australian National Audit Office, *Successful Implementation of Policy Initiatives Better Practice Guide*, October 2014, pp. 30, 34.

9 The Quality Management System was granted International Standards Organization (ISO) 9001:2008 accreditation, following an assessment by SAI Global Limited.

investment in PSAMS, the department formed the view in early 2014 that the system did not have the functionality needed for future vetting operations.

17. AGSVA has been unable to meet agreed benchmark timeframes for processing security clearances since 2010, and despite investments in people, systems and processes, there has been no noticeable improvement in the timeliness of clearance processing. In 2013–14, AGSVA completed 55 per cent of clearances within the relevant benchmark timeframe, compared to the target of 95 per cent. In March 2015, over 13 000 security clearances were overdue for revalidation—a process involving the assessment of individuals' ongoing suitability to hold security clearances. The backlog is a consequence of AGSVA using available resources to prioritise the processing of initial clearances, so as to enable employees and contractors to start work in positions that require a security clearance. The significant backlog of revalidation work requires management attention at a time of heightened government concern about the threat posed by trusted insiders.[10]

18. A key lesson of this audit is that successful implementation of a large system-level reform should be based on sound analysis and include a comprehensive risk assessment.[11] Such assessments enable government to make informed decisions on whether the reform is likely to succeed, resource requirements and the level of service which can be expected.[12] In the case of centralised vetting, implementation planning and risk management were inadequate and many significant issues emerged after AGSVA commenced operations. While investments in AGSVA's people and vetting processes have since been made, they have been of limited effectiveness in realising the expected benefits of centralised vetting.

19. Notwithstanding additional APS staff, increased utilisation of contractors and investment in ICT systems, AGSVA remains unable to meet

---

10 Trusted insiders are potential, current or former employees or contractors who have legitimate access to information, techniques, technology, assets or premises.
Australian Government, *Managing the Insider Threat to your Business, A personal security handbook,* 2014, p. 2.

11 The ANAO's *Successful Implementation of Policy Initiatives Better Practice Guide* observes that how a policy is to be implemented should be an integral part of policy design. Where implementation considerations do not receive sufficient and early attention, experience shows that problems will arise during subsequent delivery of the policy.
Australian Government, Department of the Prime Minister and Cabinet and Australian National Audit Office, *Successful Implementation of Policy Initiatives Better Practice Guide*, October 2014, p. 13.

12 ibid., p. 14.

whole-of-government vetting demand within agreed timeframes. Against this background, Defence should develop a pathway—including agreed strategies, targeted resources and a timetable—to improve its management of security vetting. Continued senior Defence management oversight, combined with a more disciplined management approach, is necessary until AGSVA's performance levels reach agreed standards. The ANAO has made three recommendations intended to promote AGSVA's delivery of more effective and timely vetting services. The recommendations involve Defence strengthening its quality assurance of vetting processes and decisions, and developing a pathway to achieve agreed timeframes for processing and revalidating security clearances.[13]

Key findings by chapter

Policy Advice and Implementation (Chapter 2)

20. The concept of centralised vetting for Australian Government entities was first raised in December 2007, and until September 2009, planning focused on the creation of a centralised vetting unit within AGD. AGD originally proposed to exempt Defence from the arrangement—which accounted for around half of all vetting activities in 2007–08—raising concerns within government about the coverage of centralised vetting and achievement of efficiencies. Defence subsequently agreed to host the centralised vetting unit by expanding its existing vetting operation to incorporate whole-of-government requirements. AGD developed a revised proposal on this basis, and in November 2009 the then Government agreed to centralise security vetting in Defence with limited exemptions. Centralised vetting was expected to increase efficiency in the vetting process, improve consistency in vetting practice, reduce delays in the transfer of clearances between entities and deliver cost savings of $5.3 million per year.

21. In a number of key areas, AGD's revised proposal to establish a centralised vetting unit within Defence was not soundly based. The proposed staffing for the centralised vetting unit represented a 25 per cent reduction

13 The audit report also suggests that Defence: consider further opportunities to align security vetting fees with the cost of specific services delivered by AGSVA; strengthen control over sensitive personnel information captured and managed as part of the security clearance process; and improve the quality of management information and reporting on AGSVA's performance. These suggestions are discussed in the key findings at paragraphs 23, 31 and 32.

compared to the reported number of vetting staff across government in 2007–08[14]; and the proposed $6.5 million contractor budget represented a 59 per cent reduction on reported contractor costs across government.[15] Further, the proposal did not consider potential risks relating to the overall reduction in resource levels; particularly how Defence would maintain vetting throughput and achieve anticipated savings. The proposal rated the overall implementation risk of centralised vetting as low on the basis that Defence already had systems and processes in place. However, Defence's core vetting systems were undergoing critical upgrades to meet internal vetting requirements, and the department had also been expending significant funds on contractors to clear large clearance backlogs.[16]

22. Defence's implementation of centralised vetting was under-resourced and AGSVA commenced operations without appropriate procedural documentation, or robust, fully functional ICT systems. AGSVA also inherited the former Defence Vetting Branch management structure which was not designed for whole-of-government work, and lacked appropriate governance and quality management arrangements. A succession of internal and external reviews conducted since AGSVA's establishment have commented on AGSVA's inability to meet expectations for efficient and effective whole-of-government security vetting, due to insufficient implementation planning, inadequate risk management and under-resourcing. In attempting to manage its workload and improve systems and processes, AGSVA's APS staffing level increased from 228 employees in October 2010 to 272 by March 2015, and its expenditure on vetting services contractors was over $17 million in 2013–14. Overall, between 2011–12 and 2013–14, AGSVA's expenditure was some 21 per cent higher than originally estimated in the November 2009 policy proposal. The additional funding was provided from within Defence's overall budget and eroded the savings anticipated from centralised vetting.

14 A Scoping Study conducted by AGD in 2008 reported 304 full-time public servants directly involved in security vetting across the Australian Government (not including other authorised vetting agencies). AGSVA was allocated 228 FTPS.

15 The reported number of centralised vetting unit staff and contractor costs in 2007–08 were based on incomplete and unverified data provided by government entities in response to the AGD Scoping Study. Fifty-three out of 164 entities (nearly one-third) invited to participate in the Scoping Study did not respond, and over half of the respondents did not answer all of the survey questions.

16 Defence reported that it spent an additional $8 million on contractors in 2007–08 to assist in clearing a backlog of revalidations.

23. To recover the cost of security vetting, Defence charges other government entities a fee for each security clearance they sponsor. The fees were introduced in 2010 and increased between 15 and 67 per cent in July 2014, indicating the charges had not been aligned with vetting costs for some time. Further, Defence did not commence charging its own contractors for security clearances until January 2015. Defence contractors could obtain a security clearance free of charge through Defence, whereas other government entities were charged for the contractor personnel they sponsored. Going forward, a more disciplined approach to the fee setting regime is required, including close tracking of vetting expenses and revenue, informing stakeholders about factors that influence vetting costs and ongoing review of charges. As the sole provider of vetting services to most government entities, there would also be benefit in AGSVA periodically reviewing its vetting methodologies, and benchmarking its activities against comparable systems to the extent practicable, with a view to identifying ways to improve efficiency and minimise charges for vetting services.

The Security Vetting Process (Chapter 3)

24. Since 2012, there have been improvements in AGSVA's administrative arrangements, policies and procedures, including its overall approach to maintaining quality in vetting operations. AGSVA's Quality Management System was accredited to an internationally recognised standard in April 2014[17], and includes security vetting policies and procedures, an internal quality audit program and quarterly management reviews. AGSVA conducted 14 internal quality audits in 2013 covering the breadth of activities carried out by its staff, which identified many areas for improvement.[18] Going forward, AGSVA needs to look beyond the milestone of gaining accreditation of its Quality Management System, and continue to support the internal quality audit function as a means to identify problems and promote continuous improvement.

25. AGSVA's security vetting process is well established and familiar to government entities that request clearances on a regular basis.[19] The vetting

17 The Quality Management System was granted International Standards Organization (ISO) 9001:2008 accreditation, following an assessment by SAI Global Limited.

18 However, a reduced internal quality audit program was undertaken in 2014. Five reports covering eight process areas were completed during 2014, and as at January 2015, two conformity audits were completed but the reports had not been finalised.

19 AGSVA's general vetting process is described at paragraph 5 and shown in Figure S.1.

process has evolved in response to the changing threat environment and advances in digital technology—AGD's 2014 update of personnel security policy included additional declarations, financial history and digital footprint checks, and AGSVA is implementing these checks in consultation with AGD. However, in 2013–14, almost one-third of clearance cases were cancelled at some point during the vetting process, with AGSVA applying considerable resources to cases that were ultimately cancelled.[20] The underlying causes of cancellations require further attention to help identify opportunities for improved efficiency.

26. Around 50 per cent of AGSVA's security clearance assessments are completed by IVP contractors under a Deed of Agreement with Defence. AGSVA conducts an informal program of visits to IVP contractors' premises, and IVP assessments are reviewed by an AGSVA Delegate as part of the decision-making process for each clearance. These arrangements provide relatively limited assurance as to whether the IVP contractors comply fully with personnel security policy and AGSVA's procedures. AGSVA had planned to implement an IVP audit program in 2014, but this has been deferred to late 2015. Implementation of the planned audit program would provide additional assurance that IVP contractors have appropriate systems and processes in place, and adhere to relevant policy and legislation.[21]

27. Over time, AGSVA has denied a relatively small proportion of security clearances.[22] AGSVA has advised that this reflects: clearance subjects having already been through employment screening processes; the cancellation of complex cases during the vetting process; and AGSVA's obligation to apply the principle of procedural fairness, which can result in mitigation of identified security concerns.[23] The low rate of clearance requests which are denied has raised a concern among some entities that security risks may not have been fully identified, or mitigated. In response to the ANAO's September 2014

20 Cancellations occur when: the sponsoring entity cancels the clearance request; the clearance subject withdraws from the vetting process; or the clearance subject fails to provide required information within a specified timeframe. In 2013–14, 15 886 cases were cancelled during the vetting process.

21 The *Personnel Security Vetting Practices Guidelines* state that vetting agencies are responsible for the conduct of any security vetting by their contracted service providers, and ensuring they comply with requirements of the Protective Security Policy Framework (PSPF).

22 Refer to Table 3.5 on page 71.

23 Procedural fairness is outlined in chapter 6 of the 2014 *Personnel Security Guidelines Vetting Practices*.

Questionnaire[24], several entities also questioned the rigour of AGSVA's assessment process. Further, an AGSVA internal quality audit in 2013 identified inconsistent additional checks at the vetting assessment and decision stages for similar clearance cases. In light of concerns expressed by stakeholders, and findings of the internal quality audit, Defence should implement a program of internal peer review of Delegate decisions, supplemented by periodic external independent quality assurance, to strengthen quality control over vetting decisions, promote consistent decision-making and strengthen confidence in the vetting process.

Management of Information Systems (Chapter 4)

28. AGSVA uses two primary information systems to process security clearances. The ePack system allows clearance subjects to complete and submit their security vetting packs through an online portal, and the system uploads clearance information directly to PSAMS.[25] In May 2008, the PSAMS Refresh Project was approved to upgrade the ePack and PSAMS systems to improve the Defence security vetting process. At that time, the ePack upgrade was expected to be completed by June 2009 and PSAMS by March 2010 at a combined cost of $4.785 million.

29. The ePack upgrade (ePack2) was released in September 2010 at a cost of $5.627 million. However, ePack2 had a large number of defects[26], resulting in many clearance subjects experiencing difficulty with the system. While AGSVA has subsequently completed a series of technical updates of ePack2, users of the system continue to experience useability, compatibility and stability issues. The ePack system is the public face of AGSVA, but remains a frustrating and difficult system for individual users to navigate. This raises efficiency and productivity issues for customer entities and the vetting process as a whole.

30. The PSAMS (PSAMS2) upgrade was eventually released in December 2012 at a cost of over $32 million.[27] Defence documentation indicates that

24 In September 2014, the ANAO issued a Questionnaire to a selected group of 30 Australian Government entities to obtain feedback on AGSVA's performance and identify areas for improvement. Twenty-three entities responded to the Questionnaire.

25 AGSVA uses PSAMS to capture security vetting information and manage vetting workflow. PSAMS interfaces with Defence's records management system, Objective, where the data is stored.

26 As at 10 September 2010, there were 58 Severity 1 defects, and 544 Severity 2 defects, which were not acceptable according to the PSAMS Refresh Project Test Strategy.

27 The combined cost of the ePack and PSAMS upgrades was $37.733 million, almost eight times the original 2008 estimate of $4.785 million.

shortcomings in project planning, insufficient application of ICT expertise and major changes in project scope to deliver whole-of-government vetting functionality requirements, contributed to the substantial increase in costs. PSAMS2 is intended to support adherence to personnel security policy by not allowing vetting personnel to progress through the vetting process without completing mandatory tasks.[28] However, the upgraded system has not delivered anticipated efficiencies. For example, there is at times a reliance on inefficient hard copy documentation processes. In addition, AGSVA's Vetting Support Centre[29] uses Microsoft Outlook to manage workflow due to limitations in the functionality of PSAMS. In February 2014, Defence identified the need for long-term and potentially significant investment in ICT solutions because PSAMS2 did not have the 'functionality needed for the future'.[30]

31. AGSVA currently manages some 349 000 security clearances and is responsible for the security, availability and accuracy of sensitive clearance data. The ANAO reviewed AGSVA's access control policies and procedures for Defence's records management system, and found no formalised policy and inconsistent practices, including instances where staff members could access clearance records beyond their 'need-to-know'. In February 2015, Defence assessed AGSVA's electronic information risk profile and identified a number of gaps in the framework of internal controls and instances of control breakdown.[31] Defence needs to strengthen its controls framework for the management of sensitive personnel information captured as part of the security vetting process.

Performance Monitoring and Reporting (Chapter 5)

32. The AGSVA *Service Delivery Charter* includes four Key Performance Indicators (KPIs) that address different aspects of vetting service delivery. One of these KPIs measures the timeliness of AGSVA's vetting process, with AGSVA aiming to complete 95 per cent of clearance cases within agreed benchmark

28 In December 2011, the Inspector General Intelligence and Security reported that AGSVA staff had engaged in inappropriate practices when entering information into PSAMS to increase throughput. PSAMS2 is designed to help prevent similar practices occurring.

29 The Vetting Support Centre manages reported changes in the circumstances of clearance holders, Annual Security Appraisals for PV clearances and revalidations.

30 Defence, Defence Committee (DC) Agendum Paper, Enterprise Risk deep dive: Australian Government Security Vetting Agency, 17 February 2014, p. 7.

31 An internal Information Management Review conducted in November 2014 also identified risks relating to AGSVA's information management systems. Seventy-three per cent of these risks were assessed as High or Extreme.

timeframes. While this is a relevant measure of AGSVA's efficiency in meeting customer demand, there is no apparent relationship between the 95 per cent target and the proportion of vetting cases that are complex, and therefore require additional information and review. The remaining KPIs do not measure the effectiveness of AGSVA's service delivery to inform management decision making. Reflecting the weaknesses in the program KPIs, public reporting on AGSVA's service delivery in the Defence Annual Report has been opaque, and has not conveyed the agency's performance in delivering whole-of-government vetting services over time. There remains scope for Defence to improve the quality of performance measures and public reporting on AGSVA's performance.

33. Since its inception in October 2010, AGSVA has been unable to meet its 95 per cent target for processing security clearances within benchmark times, with around 45 per cent of clearances in 2013–14 processed in timeframes exceeding the relevant benchmark. AGSVA has given priority to processing initial clearances to enable employees and contractors to start work in positions that require a security clearance, resulting in a backlog of some 13 000 clearance revalidations. Notwithstanding increases in staffing and contractor expenditure, and system upgrades since 2010, AGSVA has struggled to manage the demand for security vetting services. Against this background, Defence should 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.[32]

34. Twenty-three Australian Government entities provided feedback on AGSVA's service delivery in response to the ANAO's September 2014 Questionnaire. While 78 per cent of the respondents agreed that AGSVA's vetting services had improved over the past two years, respondents also raised concerns about aspects of AGSVA's performance, including the agency's lack of communication about the status of complex cases and identified security concerns for clearance subjects. Effective ongoing management of clearances is dependent on communication and information sharing between the sponsoring entity and AGSVA, including where security concerns are

32 As at 30 March 2015, AGSVA was managing a backlog of 13 175 revalidations for clearances at the current levels. In May 2014, Defence reported almost 40 000 clearances at previous levels were overdue for revalidation, and over 100 000 clearances at the previous levels have not been included in the revalidation regime.

identified such as past criminal behaviour. There would be benefit in AGSVA considering how best to provide feedback to the relevant entity on specific security concerns identified during the vetting process, to facilitate entities' supervision of affected staff.[33]

Summary of entity responses

35. The proposed audit report was provided to Defence, the Attorney-General's Department and the Australian Security Intelligence Organisation. Entities' summary responses are included below and Defence's full response is included at Appendix 1.

Defence

36. Defence welcomes the ANAO's report on the Central Administration of Security Vetting and accepts the report's three recommendations, which will strengthen and enhance the business improvement initiatives that the Australian Government Security Vetting Agency (AGSVA) is currently progressing.

37. Defence acknowledges the challenges faced when security vetting services were centralised in 2010, and that deficiencies and inaccuracies in resourcing, demand and performance estimations made at the time have impacted upon service delivery and expected efficiencies. As identified in the report, government personnel security policy has been substantially reviewed and reformed over the last two years. This has necessitated significant changes to the AGSVA's policy, systems and processes, which has also affected vetting throughput.

38. Defence also acknowledges that in the face of these challenges the AGSVA, as highlighted by the ANAO, has: continued to comply with Government security policy requirements[34]; achieved ISO 9001 accreditation of its quality management system; improved the usability of its ICT system in response to internal and customer feedback; and initiated substantial improvements to process automation. The AGSVA is also developing and implementing structured professional judgement tools to enhance quality, risk

33 Defence advised the ANAO that AGSVA seeks to strike the right balance between complying with Australian Privacy Principles (and the broader Privacy Act), and meeting its obligation under the PSPF to share information about personnel security risk with relevant entities.

34 ANAO comment: See paragraphs 3.33 to 3.40 for a summary of recent assessments of compliance with protective security policy.

identification, mitigation and management in complex and changing social and threat environments. These initiatives will improve the efficiency, effectiveness and agility of security vetting assessments and service delivery, and will ensure continued confidence in the AGSVA's delivery of the outcomes expected by Government.

39. Defence notes that in addition to the three formal recommendations, the ANAO's report makes a number of informal recommendations: consultation with stakeholders on redevelopment of Key Performance Indicators; increased information sharing with agencies where risks are identified through the vetting process; and strengthening its information management controls framework. Defence agrees with the ANAO and has independently commenced work in these areas.

Attorney-General's Department

40. The Attorney-General's Department (AGD) has protective security policy responsibility for the Australian Government as detailed in the Protective Security Policy Framework. The commentary in the ANAO audit report on Central Administration of Security Vetting does not appropriately balance the roles of the Departments of Defence and Finance with that of the Attorney-General's Department in the development of the new policy proposal.[35] In addition, the report does not adequately acknowledge the complex and contested policy space in which the centralised vetting proposal was developed.

41. AGD supports the three recommendations that will strengthen centralised vetting arrangements delivered by the Australian Government Security Vetting Agency (AGSVA). However, the report contains a number of findings, which in AGD's view should be coupled with recommendations to ensure the gaps and vulnerabilities identified in the current centralised vetting arrangements are appropriately addressed.

42. The outcomes of the ANAO audit will be used to inform AGD strategic review of the Australian Government's personnel security arrangements.

35 ANAO comment: The audit observes that AGD led the development of a 2009 policy proposal for centralised vetting, in consultation with Defence and the then Department of Finance and Deregulation.

Australian Security Intelligence Organisation

43. Significant strides have been made with the AGSVA in resolving some of the points of difference that have historically existed in the relationship. Chief amongst these was the agreement reached with the AGSVA in early 2015 for ASIO to commence its security assessment of individuals only once the AGSVA's vetting recommendation had been finalised. It is anticipated that this will significantly reduce system inefficiencies by providing ASIO with access to all information collected during the vetting process thereby reducing exchanges with the AGSVA over requests for further information, significantly improving ASIO's response timeframes, and limiting ASIO effort expended on cases that are later rejected by the AGSVA on eligibility or suitability grounds.

44. Substantial progress has also been made in recent months over the drafting of a formal ASIO/AGSVA Protocol intended to address issues raised in the ANAO report commentary regarding such matters as processing times for non-complex cases, mandatory data requirements, and ICT arrangements. It is expected this draft will be finalised by July this year and provide a robust and flexible framework for engagement.

Recommendations

Recommendation No.1

Paragraph 3.31

To provide additional assurance that AGSVA's Industry Vetting Panel (IVP) contractors are operating in accordance with applicable security policies and procedures, the ANAO recommends that Defence implement a targeted audit program to assess IVP contractors' operations.

Defence response: *Agreed*

Recommendation No.2

Paragraph3.55

To strengthen quality control over vetting decisions and promote consistent decision-making, the ANAO recommends that Defence introduce a program of internal peer review supplemented by periodic independent external quality assurance of Delegate decisions.

Defence response: *Agreed*

Recommendation No.3

Paragraph 5.39

To improve efficiency and maintain the integrity of security vetting, the ANAO recommends that Defence develop a clear pathway to achieve agreed timeframes for processing and revalidating security clearances.

Defence response: *Agreed*

Audit Findings

1. Introduction

This chapter outlines the role of the Australian Government Security Vetting Agency in the management of personnel security. It also introduces the audit objective, scope and methodology.

Background

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

1.2 Australian Government entities managed their own security vetting for employees and contractors until the end of September 2010. AGSVA was then established within the Department of Defence (Defence) from 1 October 2010 to centrally administer personnel security clearances on behalf of Australian Government entities.[36] 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 security vetting service; and cost savings of $5.3 million per year.

1.3 Most government entities must use AGSVA's security vetting service for personnel that require a clearance.[37] AGSVA's vetting process involves enquiry into, and corroboration of, a person's background, character and personal values, before a decision is made by AGSVA on whether to grant or continue a clearance.

36 Before the establishment of AGSVA, over 100 government entities were responsible for managing their own security vetting processes, and over 50 of those entities held separate contracts with vetting service providers.

37 Other authorised vetting agencies include the Australian Federal Police (AFP), the Department of Foreign Affairs and Trade (DFAT) and those Australian Intelligence Community agencies not in the Department of Defence. These agencies are responsible for conducting their own security vetting.

Australian Government Security Vetting Agency

1.4 The security vetting services provided by Australian Government Security Vetting Agency (AGSVA) to Australian Government entities[38] include: assessing individuals' applications for security clearances; managing reported changes in individuals' circumstances; and periodically assessing individuals' ongoing suitability to hold a security clearance. The AGSVA *Service Level Charter* (Charter) documents the services to be provided by AGSVA, fees payable for the services, agreed performance standards and vetting responsibilities of AGSVA and entities.

1.5 As at March 2015, AGSVA had management responsibilities for over 349 000 active Australian Government security clearances.[39] Figure 1.1 shows the number of security clearance cases finalised by AGSVA since the agency's first full year of operations. Finalised cases include those that were granted, continued, denied or revoked. It does not include clearances cancelled during the clearance process.[40] The figure shows a slight reduction in finalised cases from approximately 39 000 in 2011–12 to 33 000 in 2013–14. The reduction in finalised cases broadly corresponds with the reduction in overall Australian Public Service (APS) staff numbers in 2012–13 and 2013–14.[41]

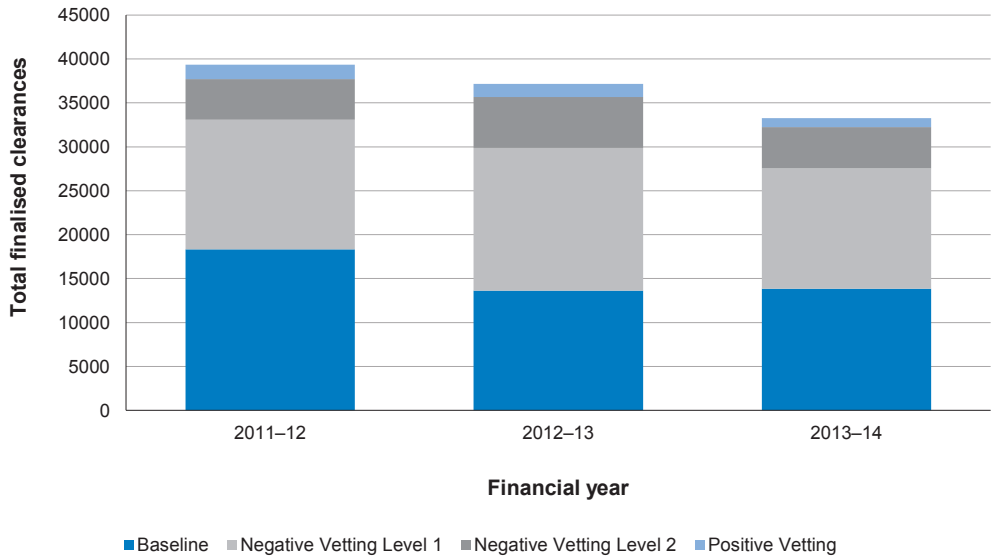
38 AGSVA may also conduct security vetting for state and territory entities, if requested.

39 A security clearance provides a level of assurance of an individual's suitability at a particular point in time. AGSVA, Australian Government entities, individual managers and individuals all have responsibilities for monitoring the ongoing suitability of an individual to hold a security clearance.

40 Cancellations refer to cases where the vetting process was ceased prior to finalisation, and occur for a range of reasons such as failure by the clearance subject to provide necessary information, or cancellation of the requirement by the sponsoring entity.

41 Australian Public Service Commission, *APS at a glance* [Internet]; available from <http://www.apsc.gov.au/publications-and-media/current-publications/aps-statistical-bulletin/aps-statistical-bulletin-2013-14/section-four#engage> [accessed 2 February 2015].

Figure 1.1: Number of security clearance cases finalised by AGSVA, by level, 2011–2014



Source: Analysis of AGSVA annual reports to Secretaries' Committee on National Security (SCNS).

Organisational structure and personnel

1.6 AGSVA forms part of Defence's Intelligence and Security Group, and is led on a day-to-day basis by the Assistant Secretary Vetting. The current organisational structure of AGSVA includes an executive group in Canberra, a National Coordination Centre in Brisbane, a Vetting Support Centre in Adelaide and regional offices in each state and territory. The National Coordination Centre conducts administrative activities, including coordinating vetting work and managing contractors. The Vetting Support Centre manages security clearance maintenance activities and the AGSVA Customer Service Centre. The regional offices are responsible for vetting assessments and determinations.

1.7 Before the launch of AGSVA, the then Defence Vetting Branch comprised 188 full-time equivalent APS staff. At the same time, the Australian Security Vetting Service (ASVS) within AGD, provided security vetting services for some government entities which did not have an in-house vetting function. In establishing AGSVA, the then Government moved ASVS functions from AGD to Defence as a Machinery of Government change, and increased Defence's civilian average staffing level by 40, including the ASVS staff. This meant that AGSVA was initially funded to have 228 APS staff. As at March 2015, AGSVA employed 272 APS staff.

The former Defence Vetting Branch used a contracted workforce to perform vetting services and supplement APS staff. AGSVA also relies on a contracted workforce to perform certain vetting assessment work and provide support services. AGSVA has three main contracting arrangements in place: the Industry Vetting Panel (IVP); the CareersMultiList (CML) contract; and contracted psychological services:

- The IVP comprises 21 companies and approximately 210 Assessing Officers (AOs).[42] Upon receipt of a request from AGSVA, the IVP AOs assess an individual's suitability to access classified resources and make a recommendation to AGSVA as to whether a security clearance should be granted.
- The CML contract is used to provide AGSVA with short-term administrative support personnel. CML personnel perform vetting support services such as checking submitted clearance packs for completeness and printing hard copy clearance packs for IVP assessment. As at February 2015, 49 CML personnel worked at AGSVA's Brisbane office and another 18 at the Adelaide office.
- AGSVA also utilises a panel of approximately 48 industry psychologists to supplement its internal psychological assessment capability as required.

ICT systems

1.8 AGSVA uses a number of Information and Communications Technology (ICT) systems to support security vetting, including the Personnel Security Assessment Management System (PSAMS), ePack and Defence's records management system, Objective:

- PSAMS is intended to be the authoritative source of all personnel security clearance data managed by AGSVA. It is used to coordinate clearance requests, track their progress and record decisions made.
- After PSAMS is used to initiate a clearance process, the clearance subject accesses the ePack questionnaire, which takes them through a

42 In May 2014, AGSVA reported that 12 of these IVP companies engaged an additional 60 subcontractors.

series of information requirements and enables the provision of most information through the Defence Online Services Domain.[43]

- After submission by the clearance subject, the ePack and supporting information is uploaded into PSAMS. Documentation relevant to the security clearance process is contained in each clearance subject's Personal Security File (PSF) and stored in Defence's records management system, Objective.

Personnel security policy and clearances

1.10 The Protective Security Policy Framework (PSPF) establishes controls for the Australian Government to protect its people, information and assets.[44] The PSPF includes: Personnel Security Core Policy, Personnel Security Protocol, Vetting Practices Guidelines, and Personnel Security Agency Responsibility Guidelines which provide detailed policy and guidance on personnel security and security vetting. A decision about granting a security clearance should be made in accordance with the standards identified in the PSPF.

1.11 The Personnel Security Core Policy aims to:

- reduce the risk of loss, damage or compromise of Australian Government resources by providing assurance about the suitability of personnel authorised to access those resources;
- create an environment where those accessing Australian Government resources are aware of the responsibilities that come with that access and abide with their obligations under the PSPF;
- minimise potential for misuse of Australian Government resources through inadvertent or deliberate unauthorised disclosure; and

43 The Defence Online Services Domain is an online gateway to access Defence applications, including the AGSVA ePack.

44 The PSPF applies to: non-corporate Commonwealth entities subject to the *Public Governance, Performance and Accountability Act 2013* (PGPA Act); corporate Commonwealth entities and companies subject to the PGPA Act that have received Ministerial direction to apply the protective security policies of the Australian Government; and other bodies established for a public purpose under a law of the Commonwealth and other Australian Government agencies, where the body or agency has received a notice from the relevant Minister that the PSPF applies to them. For further information see 'Applicability of the PSPF' in the PSPF.

- support a culture of protective security.[45]

1.12 The Personnel Security Core Policy establishes nine mandatory requirements for personnel security, which apply to Commonwealth entities, personnel and/or the entities that conduct security vetting (see Appendix 2). Under the Core Policy, vetting assessments and decisions are to take into account all available and reliable information, whether favourable or unfavourable, about the clearance subject. The Personnel Security Core Policy states that: 'Any doubt about the suitability of a clearance subject is to be resolved in favour of the national interest.'[46]

1.13 Australian Government entities must ensure that access to, and dissemination of, classified resources is restricted to those personnel who need the resources to do their work—the 'need-to-know' principle.[47] There are four levels of security clearance that allow personnel to access associated levels of classified resources. Table 1.1 outlines the clearance levels, corresponding access levels, and the reported number of active clearances for each level as at March 2015.

Table 1.1: Active security clearances, current levels, March 2015

Clearance level	Security level of accessible resources	Active clearances
Baseline	Protected	58 361
NV1	Protected, Confidential, Secret	59 696
NV2	Protected, Confidential, Secret, Top Secret	21 878
PV	All classification levels including certain types of caveated, compartmented and codeworded information.	5 346
Total		145 281

Source: AGD, *Australian Government Personnel Security Protocol*, Version 2.0, Canberra, September 2014, pp. 16–17, and ANAO analysis of PSAMS data.

1.14 The four current security clearance levels were introduced as part of the PSPF in 2010. Before that time, there were six national and non-national

45 AGD, *Australian Government Personnel Security Core Policy* [Internet], available from <http://www.protectivesecurity.gov.au/personnelsecurity/Pages/default.aspx> [accessed 24 September 2014].

46 ibid.

47 AGD, *Australian Government Personnel Security Protocol*, Version 2.0, Canberra, September 2014, pp. 4–5.

security clearance levels. Table 1.2 shows the number of clearances at previous levels which were still active as at March 2015, and their alignment with current clearance levels.

Table 1.2: Active security clearances, previous levels, March 2015

Previous clearance level	Current equivalent clearance level	Number of active clearances
Restricted and Entry[a]	No equivalent	47 430
Protected	Baseline	36 322
Highly Protected	No equivalent	13 506
Confidential	No equivalent	43 951
Secret	NV1	50 283
Top Secret Negative Vetting (TSNV)	NV2	8 327
Top Secret Positive Vetting (TSPV)	PV	4 114
Total number of active clearances		203 933

Source: ANAO analysis of PSAMS2 data.

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

1.14 Recent high profile international incidents have highlighted the importance of sound personnel security practices, and the potential consequences of inadequate vetting and employer monitoring and reporting.[48] In a speech to the 2014 Security in Government Conference, the Attorney-General stated that:

> The leaking of classified information both at home and overseas highlights the importance that our framework must remain up to date to guard against the threat posed by trusted insiders. …

48 For example, in 2013, Aaron Alexis killed twelve people and injured several others when he entered a United States (US) Navy facility with a shotgun using a security clearance which had been issued in 2008. Investigations by the US House of Representatives have found that the background check which led to the issue of the clearance failed to detect his prior history of firearms offences, and that instances of erratic behaviour after the clearance was issued had not been reported. The company which conducted Alexis' background checks was also found to have conducted the checks for Edward Snowden, who was issued with a Top Secret clearance and has since been accused of unauthorised disclosure of classified information. In January 2014, the US Justice Department filed a complaint against the company, US Investigation Services (USIS), for providing incomplete background investigations between March 2008 and September 2012.

> To address the risks that could arise from a trusted insider, the importance of security vetting, contact reporting and ongoing monitoring of our employees' suitability to access information should never be underestimated.[49]

1.16 In late 2014, AGD introduced a number of reforms to personnel security policy. The reforms are intended to clarify the responsibilities of government entities, direct resources to the areas of greatest risk and further strengthen the assessment of a person's ongoing suitability to hold a security clearance.

Audit approach

Audit objective, criteria and scope

1.17 The audit objective was to examine whether the Department of Defence provides an efficient and effective security vetting service for Australian Government entities through the Australian Government Security Vetting Agency (AGSVA).

1.18 The high-level criteria used to assess AGSVA's performance were:

- AGSVA's establishment was well planned and supported by an implementation strategy that enabled the agency to undertake the responsibilities conferred upon it;
- AGSVA has adequate guidelines, procedures and systems in place to support the security clearance process;
- AGSVA's security clearance policies and procedures comply with Australian Government policy, including the PSPF;
- AGSVA identifies areas for improvement in security clearance arrangements and implements strategies to enhance performance; and
- Defence monitors, evaluates and reports on the efficiency and effectiveness of AGSVA's security vetting service.[50]

1.19 The ANAO consulted with relevant stakeholders including Australian Government entities and industry representatives. In September 2014, the ANAO issued a Questionnaire to a selected group of 30 Australian

---

49 Senator the Hon. George Brandis QC, Attorney-General, Speech, *2014 Security in Government Conference – 'The Insider Threat'*, Canberra, 2 September 2014.

50 The audit did not assess whether individual security clearances have been appropriately granted or denied.

Government entities to obtain feedback on AGSVA's performance and identify areas for improvement. Twenty-three entities responded to the Questionnaire, and their feedback has been included in relevant sections of the audit report.

1.19 The audit was conducted in accordance with ANAO auditing standards at a cost to the ANAO of some $560 000.

Report structure

1.20 The remaining report structure is outlined in Table 1.3.

Table 1.3: Report structure

Chapter number and title	Contents
Chapter 2: Policy Advice and Implementation	Examines the development of policy advice to government on the establishment of centralised vetting arrangements; implementation planning and management for the establishment of AGSVA; and reviews and reforms of AGSVA's operations following the agency's launch.
Chapter 3: The Security Vetting Process	Examines AGSVA's management of security vetting, including oversight of the Industry Vetting Panel and compliance with protective security policy.
Chapter 4: Management of Information Systems	Examines the development and management of AGSVA's information systems and security clearance data.
Chapter 5: Performance Monitoring and Reporting	Examines AGSVA's key performance indicators and performance reporting. It also examines the timeliness of AGSVA's security vetting services and entity feedback on the agency's performance.

2. Policy Advice and Implementation

This chapter examines the development of policy advice to government on the establishment of centralised vetting arrangements; implementation planning and management for the establishment of AGSVA; and reviews and reforms of AGSVA's operations following the agency's launch.

Introduction

2.1 Before the establishment of AGSVA, Australian Government security vetting was decentralised, with over 100 government entities managing personnel security vetting based on Australian Government policy requirements. In December 2007, the then Government agreed that the Attorney-General would bring forward a cross-portfolio savings option to establish a single security vetting agency for all Australian Government security clearances. The option to establish a centralised vetting unit within AGD was explored until September 2009, at which time the Secretary of AGD agreed to discuss the possibility of Defence hosting the centralised vetting unit with the Secretary of Defence. This led to a proposal recommending the establishment of AGSVA within Defence, which was presented to the National Security Committee of the Cabinet (NSC) in November 2009. Following ministerial agreement to the proposal, Defence had ten months to prepare for the launch of AGSVA on 1 October 2010.

2.2 In this chapter, the ANAO examines:

- policy advice to government on the establishment of centralised security vetting arrangements;
- Defence's implementation planning and management for the establishment of AGSVA; and
- reviews of AGSVA's operations following the agency's launch in October 2010, and related reforms of AGSVA's structure, systems and processes.

Policy advice on centralised vetting

2.3 In reviewing the development of policy for the proposed centralised vetting unit, the ANAO focused on proposed implementation arrangements and risk management. Experience shows that a policy initiative is more likely to achieve its intended outcomes when the question of how the policy is to be

implemented has been an integral part of policy design. It is also important to inform the Government of any significant risks to implementation and proposed responses, particularly when rapid policy development and implementation are required.[51]

Vetting Review Scoping Study

2.4 As mentioned in paragraph 2.1, in December 2007, the then Government agreed that the Attorney-General would bring forward a cross-portfolio savings option to establish a single security vetting agency in place of the decentralised model operating at that time. The measure was to be considered as part of the 2008–09 Commonwealth Budget process. Subsequently, in March 2008, the then Prime Minister agreed to defer consideration of the savings option, and that AGD should undertake a cross-entity survey to identify ways to achieve efficiencies in security vetting and assess the feasibility of a centralised vetting agency.

2.5 AGD conducted the survey of Australian Government entities, referred to as the Vetting Review Scoping Study (Scoping Study), between 25 June 2008 and 9 July 2008. The Scoping Study attempted to gauge the level and cost of security vetting activity across government, and the nature of the administrative arrangements used to perform the work. Of the 164 entities invited to participate in the survey, 111 (68 per cent) responded.[52] Some of the main findings of the Scoping Study are summarised in Table 2.1.

51 Australian Government, Department of the Prime Minister and Cabinet and Australian National Audit Office, *Successful Implementation of Policy Initiatives Better Practice Guide*, October 2014, p. 13.

52 One hundred and four FMA Act agencies were invited to participate and 85 responded. Sixty *Commonwealth Authorities and Companies Act 1997* (CAC Act) bodies were invited to participate and 26 responded.

Table 2.1: Findings of the Vetting Review Scoping Study

Subject matter	Main findings[a]
Vetting activities	The survey respondents reported finalisation of 42 646 initial security clearances in 2007–08. Defence reported finalisation of 24 131 initial security clearances in 2007–08 (some 57 per cent of total initial clearances).
Vetting costs	The respondents estimated their total expenditure on the administration of security clearances for 2007–08 at $43.9 million, excluding corporate overheads. Defence reported expenses of $26.2 million in 2007–08 (some 60 per cent of expenditure).
Staff involved	The respondents reported 304 full-time public servants directly involved in the administration of security clearances. Defence reported that 154 FTPS administered its security clearance process (some 50 per cent of the total FTPS).
Staff qualifications	Thirty-seven per cent of respondents reported that their assessing officers did not hold formal security vetting qualifications.
Contractor work	Forty-eight per cent of the respondents reported use of contracted service providers for vetting activities, with some respondents relying solely on contractors. Fifty-one per cent of the respondents who used contracted service providers reported that they had no process to verify the qualifications of service provider staff.
Processing times	The reported average security clearance processing times ranged from 49 working days for Protected clearances through to 124 working days for TSPV clearances.
Transfer of clearances	Five respondents reported that they had rejected the transfer of a security clearance from another entity.

Source: AGD, Vetting Review Scoping Study, 2008.

Note a: The data in the table does not include survey responses provided by authorised vetting agencies other than Defence; specifically: the Australian Federal Police (AFP), the Department of Foreign Affairs and Trade (DFAT) and those Australian Intelligence Community agencies not in the Department of Defence.

2.6 The Scoping Study highlighted a number of inefficiencies in decentralised security vetting arrangements, including over 50 government entities managing separate contracts with vetting service providers, and entities not accepting the transfer of security clearances granted by other government entities. The Scoping Study also identified shortcomings in administrative arrangements, including that many entities employed staff with no formal vetting qualifications, did not verify the qualifications of contracted personnel performing vetting work and/or did not adequately oversee vetting work performed by contractors. These findings provided a basis for subsequent advice to government on the benefits of establishing a centralised vetting agency.

2.7 While the Scoping Study provided useful information on security vetting activities and costs for the respondents during 2007–08, it did not establish the total number and cost of vetting activities across government. In particular, 53 out of 164 entities (nearly one-third) invited to participate in the survey did not respond, and over half of the respondents did not answer all of the survey questions.[53] Further, entities self-assessed their vetting activities, costs and arrangements, and the data they provided was not independently validated, even on a sample basis.

Proposal for a centralised vetting unit within the Attorney-General's Department

2.8 Following completion of the Scoping Study, in early 2009, AGD commenced development of a proposal to centralise government security vetting and provide 'whole-of-government' security clearances. The proposal involved the establishment of a centralised vetting unit within AGD, with the majority of the work to be contracted out to a panel of service providers, managed by the centralised vetting unit.

2.9 Under the AGD proposal, certain law enforcement and intelligence entities were to be exempted from centralised vetting due to the sensitive environment in which they operated. Further, Defence was to be exempted due to concerns that the centralised vetting unit could not manage the high volume Defence vetting workload, and on the basis that Defence already had the infrastructure and systems in place to perform this work in the most efficient manner. The exclusion of Defence, and the high start-up costs faced by AGD in the establishment of a centralised vetting unit, initially reduced its ability to identify significant cost savings.

2.10 The proposal was considered by the Secretaries' Committee on National Security (SCNS) in September 2009, which requested further work to address concerns raised by some entities regarding the proposed business model. The proposal to exempt Defence, which accounted for around half of vetting activities in 2007–08, brought into question the achievement of efficiencies under the proposed business model. In other words, to achieve the benefits associated with centralisation, AGD needed to develop a model which included Defence.

---

53 In a number of fields related to general expenses or corporate overheads, many respondents answered $0 or that the expenses were 'corporately funded'.

Proposal for a centralised vetting unit within Defence

2.11 Notwithstanding an initial reluctance to host a centralised vetting unit, following a request from the Secretary of AGD in September 2009, Defence agreed to do so by expanding its existing vetting operation to manage whole-of-government requirements.

2.12 In November 2009, Ministers agreed to centralise security vetting in Defence, with limited exemptions[54], on the basis of a revised proposal developed by AGD in consultation with Defence and the then Department of Finance and Deregulation. The centralised vetting unit was to be the authority for granting and revalidating security clearances, which would have automatic application across the Australian Government, except for other authorised vetting agencies. Introduction of centralised vetting was expected to increase efficiency in the vetting process, improve consistency in vetting practice, reduce delays in the transfer of clearances and deliver cost savings of $5.3 million per year.

2.13 However, in a number of key areas, the revised proposal was not soundly based. In particular, there were shortcomings relating to vetting resource requirements and costs savings, and implementation readiness and risks. AGD informed the ANAO in May 2015 that the revised proposal was developed in the context of a complex and contested policy space.

Centralised vetting resources and cost savings

2.14 The identification of potential savings from centralised vetting depended on the methodology used to calculate cost estimates, and the assumptions made about vetting activity and future resource requirements. Cost estimates for the revised proposal were calculated as follows:

(a) Firstly, the overall annual cost of decentralised vetting activity was estimated at $43.9 million, based on the Scoping Study survey responses.

(b) Secondly, the estimated annual cost of centralised vetting activity within Defence was derived using a Defence cost modelling tool and the Department of Finance and Deregulation 2010–11 costing template for personnel finance.

54 Authorised vetting agencies (other than Defence) were exempted from the centralised vetting arrangement.

(c) Two key assumptions were made: that the level of vetting activity undertaken by the proposed centralised vetting unit would be similar to that reported by entities for 2007–08; and that the unit would comprise 228 staff. The total cost of vetting activities by a Defence centralised vetting unit was estimated to be $38.6 million.

(d) The difference between $43.9 million and $38.6 million was used to estimate the annual cost saving arising from the move to centralised vetting—some $5.3 million.

2.15 The cost estimates relied on incomplete and unverified data from the Scoping Study. As discussed, nearly one-third of entities did not respond to the Scoping Study survey and many respondents did not answer all questions related to expenses. However, the revised proposal placed no caveats on the $5.3 million savings figure.

2.16 The proposed number of centralised vetting unit staff (228) represented a 25 per cent reduction on the reported number of vetting staff across government for 2007–08. Further, the revised proposal was based on conducting the majority of vetting activity in-house, whereas around half of the survey respondents had reported using contractors to process clearances.

2.17 The Scoping Study identified contractor costs under decentralised vetting arrangements of $15.9 million for 2007–08. In contrast, the revised proposal estimated centralised vetting unit contractor costs at $6.5 million, which was a reduction of $9.4 million (59 per cent). The proposal did not address how the proposed Defence centralised vetting unit would manage the volume of whole-of-government vetting activity without increased reliance on external vetting contractors.

2.18 The revised proposal did not consider potential risks relating to the overall reduction in resource levels; particularly how Defence would maintain vetting throughput and achieve anticipated savings. In the event, the number of staff employed by AGSVA has increased over time—as at March 2015, AGSVA employed 272 staff, compared to 228 in October 2010. In addition, AGSVA has continued to rely heavily on a range of contracted personnel to perform vetting and support activities. In 2013–14, the IVP conducted approximately 90 per cent of vetting assessments for NV1 and NV2 clearances and approximately 15 per cent of PV clearances, at a cost of approximately $12.8 million; and AGSVA's total expenditure on vetting services contractors in 2013–14 was some $17 million.

Implementation readiness and risks

2.19 The revised proposal rated the overall implementation risk for the proposed centralised vetting arrangement as 'low', and it was presented as an efficient option using an ongoing vetting operation in Defence that already processed the majority of government security clearances. The proposal noted that Defence had a strong record managing a high volume vetting workload, and start-up costs would be minimised because Defence already had the necessary infrastructure, technology, personnel and expertise. The proposal did not mention that Defence had experienced significant backlogs in the completion of its own security vetting.

2.20 In addition, the revised proposal did not mention that Defence's two primary security vetting processing systems—PSAMS and ePack—were undergoing critical upgrades to meet vetting requirements. Defence had identified the importance of these upgrades as early as 2007:

> By not improving the technology used within the vetting processes, [the Defence Security Authority] will be unable to meet current and future demand for security clearances. This will impact on the Department in extended recruitment times, higher risk of a major security breach and continued bad publicity for the department in regards to its clearance process.[55]

2.21 The system upgrades were initially combined and known as the 'PSAMS Refresh Project'. The August 2009 Project Plan identified a number of risks and issues which had the potential to affect Defence's readiness for centralised vetting on the proposed establishment date. Ultimately, both of the system upgrades encountered major difficulties, which are discussed later in this chapter and in chapter 4.

2.22 At the time the revised proposal was put to government (November 2009), significant changes to protective security policy were planned. The PSPF was released in June 2010, replacing the Protective Security Manual (PSM). The changes brought about by the PSPF included the introduction of revised national security clearance levels (refer to Table 1.2), mandatory periodic review periods for all security clearance levels[56], and mandatory competencies for security vetting practitioners.

---

55 Defence, Defence Information Environment Project Mandate Proposal, October 2007, Hurt Statement, p. 3.

56 Previously, recommended review periods for security clearances below Secret level were not consistently applied.

2.23 The revised proposal suggested that the centralised vetting unit start date be delayed from July 2010 until October 2010, to give Defence sufficient time to respond to the protective security policy changes by amending its IT systems to support vetting under the revised security clearance levels. However, the revised proposal did not consider any other potential implications of prospective changes to personnel security policy for the centralised vetting unit's operations. For example, it did not consider the potential need to:

- align existing security clearances with the new clearance levels;
- process security clearance revalidations for all clearance levels in specified timeframes; and
- train the vetting workforce to meet mandatory competencies.

Purchaser-provider arrangement

2.24 The main risk identified in the revised proposal was that the Defence centralised vetting unit may be inefficient and unresponsive. This risk was to be mitigated through a rigorous and transparent purchaser-provider arrangement and performance reporting.

2.25 Purchaser-provider arrangements have been adopted by many public sector organisations in recent decades. These arrangements separate the 'purchaser' from the 'provider' of public services in order to increase the efficiency and effectiveness of service delivery.[57] In the Australian Government context, purchaser-provider arrangements have been used to draw on the experience of entities that have specialised delivery skills.

2.26 Under the proposed centralised vetting purchaser-provider model, Defence was to charge other government entities the cost of processing clearances.[58] This arrangement was intended to mitigate the risks of over or under funding of the central vetting unit. The intent was also to send a clear

57 A purchaser-provider arrangement is normally formalised through a contract, service level agreement or memorandum of understanding, which identifies the desired outcomes, roles and responsibilities, governance mechanisms, resourcing, review mechanisms, risk management approaches, performance information, and monitoring and reporting mechanisms. In general terms, when negotiating an arrangement, key considerations for the purchaser include setting outcomes and priorities, funding arrangements (including any pricing mechanisms), and performance measures. In turn, providers generally have a degree of autonomy in delivering services to achieve specified outcomes.

58 Defence allocates resources to AGSVA for its own security vetting services but is not notionally charged by AGSVA for individual clearances.

message (price signal) to customers about the actual cost of resources involved in security vetting. Charges were to be updated annually and approved by the Secretary of Defence in consultation with the then Department of Finance and Deregulation.

2.27 AGSVA's fees were incorporated in its Charter in August 2010. The fees remained unchanged until July 2014, when increases of 15 to 67 per cent for initial clearances and 15 to 30 per cent for revalidations were made (refer to Table 2.2). The significant fee increases indicate that charges were not well aligned with the cost of security vetting for some time.

Table 2.2: AGSVA fee increases

Clearance level	Initial clearance		Revalidation	
	2010 ($)	2014 ($)	2010 ($)	2014 ($)
Baseline	333.67	394.46	133.58	157.78
NV1	637.68	1067.22	255.06	426.89
NV2	1757.71	2023.12	703.25	809.25
PV	6791.73	8967.31	5432.80	7173.58

Source: Department of Defence, *AGSVA Service Level Charter*, 5 August 2010; and Department of Defence, *AGSVA Service Level Charter*, 1 July 2014.

2.28 Until recently, Defence contractors could obtain a security clearance free of charge through Defence, whereas other government entities were charged for the contractors they sponsored. On 1 January 2015, AGSVA commenced charging Defence industry providers and contractors for security vetting services, indicating that: 'All revenue raised—estimated at $7–10 million per annum—will be used to build vetting capacity and enhance service delivery.'[59]

2.29 Recent fee increases have been significant, and going forward, a more disciplined approach to the fee setting regime is required, including: close tracking of vetting expenses and revenue; informing stakeholders about factors that influence vetting costs; and ongoing review of charges. As a sole provider of vetting services to most government entities, there would also be benefit in AGSVA periodically reviewing its methodologies, and benchmarking its activities against comparable systems to the extent practicable, with a view to identifying ways to improve efficiency and minimise charges.

59 AGSVA Media Release, *Advice to Defence industry: Defence to charge industry for security vetting services from 1 January*, 20 August 2014.

Implementation planning and management

2.30 The successful implementation of a new policy initiative requires sound implementation planning and management:

> In situations where timeframe imperatives have curtailed the consideration of implementation issues during policy development, the risk to successful implementation 'down the track' increases markedly. One of the most pressing priorities for the senior responsible officer is to promptly reduce this risk by seeking expert implementation advice and experience as soon as possible in the delivery phase. …
>
> Successful implementation relies on the identification and management of risk. A robust risk management framework will promote accurate, well-informed judgements and mitigation strategies. The analysis of risks should commence as the policy is being developed and should continue through the implementation process.[60]

2.31 Following the November 2009 decision to establish AGSVA with a commencement date of 1 October 2010, Defence developed governance arrangements and implementation plans for the project. AGSVA was established within Defence's Intelligence and Security Group under the control of the Chief Security Officer. An Assistant Secretary Vetting was appointed and a Project Implementation Team established to facilitate the transition from the then Defence Vetting Branch to AGSVA. A Steering Committee was also established to oversee the transfer of the Australian Government Security Vetting Service (ASVS) from AGD to Defence under a Machinery of Government change.

2.32 The Project Implementation Team developed several planning documents between February and April 2010 including: the Introduction into Service Plan for the Australian Government Security Vetting Agency; the Australian Government Security Vetting Agency Project Plan; and the Australian Government Security Vetting Agency Change Management Strategy. These plans identified a substantial body of work to be completed before the commencement of AGSVA's operations. Key tasks included:

- the development of standard operating procedures and directives for the new organisation;

60 Australian Government, Department of the Prime Minister and Cabinet and Australian National Audit Office, *Successful Implementation of Policy Initiatives Better Practice Guide*, October 2014, pp. 17 and 29.

- business and financial model development;
- development and finalisation of service level agreements with other Australian Government entities;
- staff recruitment, transfers and training;
- significant upgrades to ePack and PSAMS;
- the creation of new external provider contracts and development of contract management arrangements; and
- testing of the AGSVA business model.[61]

2.33 Defence's Project Plan identified seven project risks, including that a Defence revalidation backlog would not be cleared, the new ePack system would not be operational[62], and modification of PSAMS to support the processing of clearances at the revised levels would not be completed by AGSVA's commencement date of 1 October 2010. However, in planning for AGSVA's implementation, Defence did not identify any risks arising from: the development of new operating procedures for whole-of-government vetting; protective security policy changes, including mandatory clearance review timeframes, and staff competencies; or the scale and complexity of implementation work, including the transfer of clearance data from other government entities. Experience has demonstrated that these were significant risks associated with the transition to centralised vetting and more could have been done to analyse and treat implementation risks.

2.34 Adding to the challenge, Defence lacked expertise in the delivery of whole-of-government services. Internal concerns were subsequently expressed that Defence's implementation arrangements were not suited to respond to the scale and complexity of the task. By way of example, a 2011 Inspector-General of Intelligence and Security (IGIS) inquiry into allegations of inappropriate vetting practices within Defence stated:

> I am advised that the oversight and implementation of [the ePack upgrade] was managed by the same team that had responsibility for the significant task

61 Defence, Intelligence and Security, Introduction into Service Plan for the Australian Government Security Vetting Agency (AGSVA), pp. 5 and 6–7.

62 The ePack upgrade, known as ePack2 was released in September 2010.

of planning for and implementing the transition of the Vetting Branch to the AGSVA. This arrangement does not seem to have been fully effective.[63]

2.35 AGSVA commenced operations on 1 October 2010 without a comprehensive, centrally managed set of procedural documentation or robust, fully functioning ICT systems. It also inherited the Defence Vetting Branch management structure which was not designed for whole-of-government work, and lacked adequate governance, oversight and quality management processes. Weaknesses in the overall model and implementation planning were identified in subsequent reviews.

Post implementation reviews and reforms

2.36 A number of reviews have been conducted since AGSVA was established, including:

- Inquiry into Allegations of Inappropriate Vetting Practices in the Defence Security Authority and Related Matters, by the Inspector-General of Intelligence and Security (IGIS), December 2011;
- Review of the Processes and Management Arrangements Supporting Australian Government Security Vetting (also known as the 'Colley Review'), January 2012;
- Organisational Analysis of the Australian Government Security Vetting Agency, undertaken by Mercer Pty Ltd for Defence's Chief Security Officer, September 2012;
- four Defence internal audits of AGSVA, including three annual reviews of AGSVA's compliance with government vetting policies in response to a recommendation of the IGIS inquiry;
- an assessment of AGSVA resourcing by Remote Pty Ltd in 2013; and
- an enterprise risk deep dive assessment of AGSVA, presented to the Defence Committee in February 2014.

2.37 The focus, key conclusions and recommendations of these reviews are discussed in the following sections.

63 Inspector-General of Intelligence and Security, *Inquiry into Allegations of Inappropriate Vetting Practices in the Defence Security Authority and Related Matters*, 2011, p. 42. The review is discussed at paragraphs 2.38–2.41.

Inquiry into Allegations of Inappropriate Vetting Practices

2.38 On 16 May 2011, ABC television's *Lateline* program aired allegations made by three former contractors who had worked at the Defence Security Authority's (DSA) National Coordination Centre in Brisbane. They made a series of allegations about inappropriate vetting practices, including 'falsifying' the information relating to clearance subjects to 'get the numbers up'.[64] The former contractors alleged that they were encouraged to make unapproved changes when entering information from submitted security packs into PSAMS to increase the volume of security clearances processed.

2.39 On 29 May 2011, the then Prime Minister requested that the IGIS conduct an inquiry into the *Lateline* allegations. The resulting December 2011 IGIS report confirmed the allegations and identified a number of factors that led to these practices, including:

- delayed and inadequate systems upgrades;
- inadequate formal documentation and manuals;
- inadequate training for contractors and APS staff;
- the use of delegates who had not completed formal qualifications;
- poor systems and process change management;
- inadequate quality assurance;
- inadequate management oversight and contractual arrangements; and
- sustained pressure for vetting output following increases in demand.

2.40 The IGIS report made 13 recommendations, which were all agreed to by the then Government. The recommendations addressed wide ranging aspects of AGSVA's administration, including the need to:

- appropriately document business processes, policies and procedures;
- professionalise the vetting workforce;
- implement a Quality Management System;
- provide appropriate management oversight of contracted personnel;

64 The modification of individuals' security pack data was found to include practices to enable the process to proceed to an Australian Security Intelligence Organisation (ASIO) security assessment. ASIO security assessments form part of the clearance process for all clearances at or above NV1 level.

- review the adequacy of staffing numbers; and
- assign high priority to the implementation of PSAMS2.

2.41 A September 2014 Defence internal audit concluded that 11 of the 13 IGIS recommendations had been implemented, with two recommendations relating to staff training yet to be fully implemented.

Defence Security Vetting Review (Colley review)

2.42 The Colley review focused on the development of AGSVA's management arrangements and work practices, and recommended 16 actions. The review report concluded in January 2012 that:

> Progress in the review and the implementation of [the review's] recommendations has been slower than expected, primarily because the work required to help bring the current AGSVA work instructions up to a fit for purpose standard has been more extensive than envisaged, the extensive remediation task faced by AGSVA, and a limited pool of subject matter experts.
>
> … a comprehensive, fit for purpose set of documentation for current business processes is unlikely before the end of 2012.[65]

Organisational analysis

2.43 An organisational analysis of AGSVA was undertaken by external consultants during 2012. The aim of this work was to develop the most appropriate future structure and staffing model for AGSVA to support the anticipated demand for vetting services across Australia.[66]

2.44 The outcomes of the organisational analysis were reported in September 2012, and included the following recommendation:

> … a reconsideration of AGSVA permanent staffing requirements given the analysis. It is understood that there are political considerations in requesting

65 Defence, Review of the Processes and Management Arrangements Supporting Australian Government Security Vetting, January 2012, p. 8.

66 The analysis indicated that AGSVA required 322 full-time equivalent APS staff, as well as IVP support to the value of $8.4 million per annum. This represented an increase of 96 FTE over AGSVA's then FTE cap of 226 staff, and a reduction in expenditure on IVP contractors of approximately $6.6 million. The report also noted that 'In the short term, it is anticipated that up to an additional 27.5 FTE are required for special projects and to address the current backlog in vetting actions.'

Mercer, Australian Government Security Vetting Agency Organisational Analysis Services, September 2012, p. 6.

> additional [staff], however an appropriately sized workforce is required for a sustainable structure, maintaining internal vetting capability, reducing risk and reducing overall staffing costs. Mercer also recommends minimising the amount of vetting assessment work that is outsourced to IVP as this has the potential to erode internal capability, poses greater risks and quality management issues, and is overall a more costly approach.[67]

Defence internal audits of AGSVA

2.45 Recommendation No.3 of the December 2011 IGIS report, referred to above, was that:

> The Defence Chief Audit Executive should review and report annually on the AGSVA's compliance with all applicable Government security vetting policies, with the first review to be completed by 30 June 2012. The results of the reviews should be reported in Defence's annual report. The need for annual reviews should be reconsidered after three years.[68]

2.46 Defence's Chief Audit Executive completed three internal audits of AGSVA, in June 2012, August 2013 and September 2014.[69] The audits reviewed AGSVA's compliance with government security vetting policy, implementation of the IGIS report recommendations and the progress of the associated AGSVA reform agenda. Defence completed a fourth internal audit in July 2014, which examined financial management in AGSVA.

2.47 The 2012 Defence internal audit concluded that AGSVA was not fully compliant with government security vetting policy. The related 2013 and 2014 internal audits found that AGSVA complied with a limited selection of policies subject to audit review. As mentioned in paragraph 2.41, the September 2014 internal audit also indicated that AGSVA had implemented 11 of the 13 IGIS report recommendations, and that further work was required for all vetting staff to hold mandatory qualifications and to finalise ongoing training for staff.

Assessment of AGSVA resources

2.48 During 2013 external consultants completed a review of AGSVA's resources and developed options for resourcing AGSVA through to 2015–16. The review report concluded that:

---

67 ibid.

68 Inspector-General of Intelligence and Security, *Inquiry into Allegations of Inappropriate Vetting Practices in the Defence Security Authority and Related Matters*, 2011, p. 6.

69 Refer to paragraph 3.37 for further discussion of the internal audits.

> From its inception AGSVA has struggled to manage the volume of work. Since December 2010 through to November 2013 it has failed to meet its key performance indicator for clearance completion times in every month. In 2012–13 19 per cent of new clearance requests and 42% of revalidation and review for cause requests completed exceeded the benchmark completion times. AGSVA has managed to contain the backlogs for new clearances by deferring revalidations.
>
> The fundamental issue is that since its establishment, AGSVA has had insufficient resources to enable the workload to be processed in sufficient time to meet performance benchmarks and to ensure that revalidations are completed within the timeframes mandated by government policy. Difficulties in managing the volume of work predate the establishment of AGSVA. AGSVA's predecessor the Defence Vetting Branch had difficulty in managing the volume of Defence work and backlogs in revalidations occurred on a regular basis.[70]

2.49 The report noted that without supplementary resources, the backlog of revalidations would grow rapidly and that Australian Government entities 'will be carrying an increasing level of risk associated with staff that access highly classified material'.[71]

2.50 The consultants also observed that the implementation of PSAMS2 in December 2012 did not appear to have resulted in the anticipated business benefits in terms of AGSVA's productivity, stating that:

> Improving the performance of PSAMS2 will increase productivity by a relatively small percentage in absolute terms. Streamlining work processes may yield productivity gains in excess of those that will be achieved by improving PSAMS2 performance.[72]

70 Remote Pty Ltd, AGSVA Resourcing 2014–15, 2013, p. 1.

71 ibid., p. 15. At the time of the review, AGSVA had a notional allocation of 247 staff in 2013–14, 221 in 2014–15 and 209 in 2015–16. The review recommended an increase in AGSVA's staffing to 279 for 2014–15, and extensive use of contractors to assist in addressing the revalidation backlog.

72 ibid., p. 6.

AGSVA enterprise risk deep-dive

2.51 One of seven key enterprise risks identified by the Defence Committee and included in the 2012–17 *Defence Corporate Plan* is:

> The Australian Government Security Vetting Agency (AGSVA) does not meet Government security vetting needs, leading to clearance delays and whole-of-government/operational capability disruptions.[73]

2.52 In 2013, an enterprise risk 'deep-dive' for AGSVA was finalised to detail the risk and control profile for AGSVA, and reach agreement on a program of action to minimise risk exposure.

2.53 The enterprise risk deep-dive recognised progress made to that time and achievements of AGSVA's internal reforms, including the establishment of procedural documentation, introduction of an internal quality audit program, training initiatives, and the introduction of PSAMS2. However, the risk assessment also indicated that AGSVA's business exposure to performance failure remained 'very high' because it did not have the business model, funding arrangements or workforce to meet the demand for vetting services on a sustainable basis.

2.54 A paper on the enterprise risk deep-dive was presented to the Defence Committee in February 2014. The authors noted that AGSVA did not have the capacity to address backlogs in clearance revalidations, leading to increased risk of misuse of government resources by the trusted insider. The paper contained five recommendations to minimise AGSVA's risk exposure:

- AGSVA and the Chief Information Officer Group assess the risk exposure of transitioning to a fully electronic vetting workflow management system;
- additional FTE allocated to AGSVA for reform implementation be sustained through 2014–15;
- AGSVA resource issues be referred to the Defence First Principles Review[74];

73 Defence, *Defence Corporate Plan*, 2012–17, p. 15.

74 The Defence First Principles Review, released 1 April 2015, does not specifically refer to AGSVA, its responsibilities for security vetting, or its resourcing position. However, the report did recommend that the Defence Security Authority, which is responsible for AGSVA, be repositioned under the control of a new position of Associate Secretary. The Government agreed to implement this recommendation.

- AGSVA lead the concept development of a 21st century vetting capability; and
- AGSVA provide an updated deep-dive risk assessment to the Defence Committee in nine months.[75]

2.55 The updated deep-dive risk assessment was presented to the Secretary and Chief of the Defence Force Advisory Committee (SCAC) in March 2015. SCAC was advised that:

> The last deep dive into AGSVA enterprise risk completed in February 2014 identified one fundamental issue: that the AGSVA was not able to meet the demand for new security clearances. A second fundamental issue has been confirmed: the AGSVA is not able to meet the revalidation requirements for existing security clearance holders.[76]

2.56 While AGSVA's deep-dive risk assessment referred to various intended actions, it did not identify a clear pathway to improve AGSVA's performance and achieve agreed timeframes for processing and periodically reviewing security clearances. The paper instead contained process recommendations, proposing that SCAC:

- note: the DSA was working to continue the provision of additional staff allocated to AGSVA in 2014–15;
- note: AGSVA was closely involved in the AGD-led Personnel Security Strategic Reforms; and
- agree: AGSVA return to SCAC with an updated deep-dive assessment in 12 months.

75 Defence, Defence Committee (DC) Agendum Paper, Enterprise Risk deep-dive: Australian Government Security Vetting Agency, 17 February 2014, p. 1.

76 Defence, Secretary and Chief of the Defence Force Advisory Committee Agendum Paper SCAC 23/2015, 10 March 2015, p. 4. The updated deep-dive also identified issues relating to a backlog of Australian Security and Intelligence Organisation (ASIO) security assessments, lack of a disaster recovery plan for ICT systems, difficulty in filling vacant positions and AGSVA's non-compliance with Defence Information Management policy.

Conclusion

2.57 The mixed performance of centralised vetting has its roots in an inadequate policy proposal developed in 2009 by AGD in consultation with Defence and the then Department of Finance and Deregulation, which did not effectively assess Defence's capacity to deliver whole-of-government services with the resources proposed. AGSVA commenced operations with significantly reduced vetting resources compared to those previously deployed across government, and without an appropriate management structure, documented procedures and adequate ICT systems. The failure to identify and address key risks during the policy development and implementation planning phases has had lasting consequences for AGSVA's delivery of vetting services.

2.58 A succession of internal and external reviews conducted since AGSVA's establishment have commented on AGSVA's inability to meet expectations for efficient and effective whole-of-government security vetting, due to insufficient implementation planning, inadequate risk management and under-resourcing. Notwithstanding additional APS staff and increased utilisation of contractors, Defence's enterprise risk deep-dive, presented to the Defence Executive in March 2015, again identified that AGSVA was unable to meet whole-of-government vetting demand within agreed timeframes. Against this background, Defence should develop a pathway—including agreed strategies, targeted resources and a timetable—to improve AGSVA's performance against benchmark timeframes, and address the revalidation backlog. Continued senior Defence management oversight, combined with a more disciplined management approach, is necessary until AGSVA's performance levels reach agreed standards.

3. The Security Vetting Process

This chapter examines AGSVA's management of security vetting, including oversight of the Industry Vetting Panel and compliance with protective security policy.

Introduction

3.1 Personnel security is a shared responsibility of Australian Government entities, agencies that conduct security vetting, individual managers and clearance holders. AGSVA's security vetting process is an important risk mitigation activity intended to protect the national interest, which can also effect an individual's employment and the business operations of entities if not managed effectively or in a timely manner. AGSVA's vetting process is derived from the Personnel Security Vetting Practices Guidelines, which provides guidance for vetting agencies in determining the suitability of personnel to access classified resources. The Guidelines specify minimum standards and checks to be conducted by vetting agencies.

3.2 This chapter commences with an overview of AGSVA's security vetting process. The chapter then examines AGSVA's:

- management of the Industry Vetting Panel (IVP);
- compliance with protective security policy; and
- vetting assessments and decisions.

Overview of the security vetting process

3.3 As discussed in chapter 2, successive reviews have indicated that AGSVA did not have adequate governance arrangements and documented processes when the agency commenced operations. The December 2011 IGIS report recommended that AGSVA document business processes and procedures, implement a Quality Management System to cover the full range of security clearance processes, and strengthen quality assurance.

3.4 AGSVA implemented a revised organisational structure during 2012. The new structure established functional teams to perform administrative and support activities, and director positions responsible for quality management, policies and procedures, vetting operations and governance arrangements.

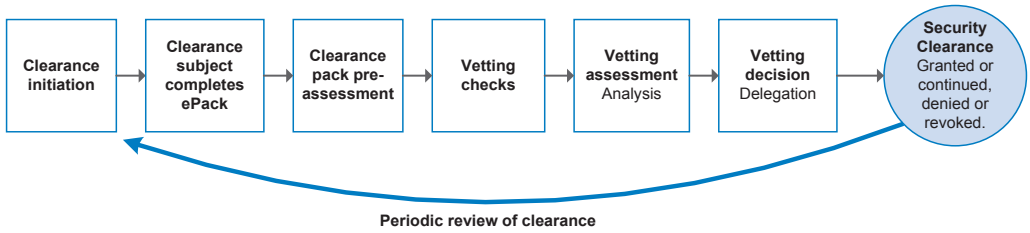
3.5 From 2012, AGSVA began introducing new security vetting policies, procedures and work instructions as part of a Quality Management System.

The documents provide high-level policy, guidelines and broad procedural information for each part of the security vetting process[77], and more detailed information on specific processes, such as managing workflow within PSAMS. AGSVA staff interviewed by the ANAO demonstrated knowledge of procedures relevant to their job and where to locate further information.

3.6 AGSVA's Quality Management System was granted International Standards Organization (ISO) 9001:2008 accreditation in April 2014. This means that the system has achieved an internationally recognised standard for an efficient quality management system, as assessed by SAI Global Limited. The Quality Management System comprises AGSVA's vetting policies and procedures, an internal quality audit program and quarterly management reviews.

3.7 Figure 3.2 illustrates AGSVA's security vetting process. The following sections discuss different stages of the process.

Figure 3.1: Overview of the security vetting process



Source: ANAO analysis of AGSVA documentation and processes.

Clearance initiation

3.8 Security clearances are required only for individuals who, as part of their work for the Australian Government, need to access classified resources. Australian Government entities request that AGSVA undertake a security vetting process for employees and contracted personnel that they sponsor. AGSVA is also responsible for initiating periodic reviews of existing security clearances in accordance with mandated review timeframes.

77 For example, AGSVA's Policy and Procedure Document 2:3 Vetting Checks explains how AGSVA personnel should conduct mandatory checks and determine whether supplementary checks are required.

Clearance subject completes ePack

3.9 After AGSVA commences a new security clearance process or a periodic review, the clearance subject receives notification to provide mandatory information using the ePack system and supporting documentation. AGSVA issues reminders to the individual to complete the request within a set timeframe.

Clearance pack pre-assessment

3.10 Clearance pack pre-assessment involves AGSVA checking the clearance subject has submitted all information and documentation required by the Assessing Officer (AO) to conduct an assessment. Where necessary, AGSVA will request additional information and await receipt before allocating the case to an AO.[78] Pre-assessment coordination also involves the initiation of some external checks, such as a police records check.

Vetting checks

3.11 Minimum personnel security checks for initial clearances vary according to the level of clearance sought (Table 3.1). The blue cells indicate new checks introduced as part of the September 2014 Personnel Security Protocol.

Table 3.1: Minimum personnel security checks for initial clearances

Baseline Vetting	NV1	NV2	PV[a]
Qualification verification	Qualification verification	Qualification verification	Qualification and documentation verification
Professional referee check	Referee checks (including one professional)	Referee checks (including one professional and one un-nominated)	Referee checks (including one professional and one un-nominated)
Police records check	Police records check	Police records check	Police records check
Financial history check	Financial history check	Financial history check	Financial history check
Five year background check	10 year background check	10 year background check	Whole of life background check
Official secrets declaration	Official secrets declaration	Official secrets declaration	Official secrets declaration

78 If the necessary information is not received after three requests, the clearance process may be cancelled.

Baseline Vetting	NV1	NV2	PV[a]
Statutory declaration	Statutory declaration	Statutory declaration	Statutory declaration
Identity verification	Identity verification	Identity verification	Identity verification
	ASIO assessment	ASIO assessment	ASIO assessment
	Suitability screening questionnaire	Suitability screening questionnaire	Suitability screening questionnaire
	Financial questionnaire	Financial questionnaire	Financial questionnaire and supporting documents
	Digital footprint checks	Digital footprint checks	Digital footprint checks
		Security interview	Security interview
			Financial probity check
			Psychological assessment

Source: AGD, Australian Government Personnel Security Protocol, Version 2.0, September 2014, p. 31; and AGD, Personnel Security Practitioners Guidelines, September 2010, p. 58.

Note a: Prior to the introduction of the revised Personnel Security Protocol in September 2014, the minimum checks for PV clearances were not specified.

Note b: When AGSVA cannot complete the minimum checks, a clearance subject is considered to have an 'uncheckable background'.

3.12 The changes made to minimum personnel security checks have resulted in additional work for AGSVA. For example, the expanded requirement for 'digital footprint checks' is an additional AO task for clearances at the NV1 and NV2 level. AGSVA informed the ANAO in February 2015 that it is updating vetting policies and procedures to cover the revised minimum checks.

Vetting assessment

3.13 AOs are responsible for the analysis of a clearance subject's suitability to hold a security clearance.[79] An AO can be an AGSVA employee or an IVP contractor. An AO analyses the information provided by the individual and the results of checks undertaken, and requests further information and conducts interviews as necessary, based on AGD's Vetting Practices Guidelines. The AO

79 Vetting assessments are to be based on a range of factors, including: external loyalties and associations; personal relationships; financial considerations; alcohol and drug usage; criminal history; attitude to security; and mental health.

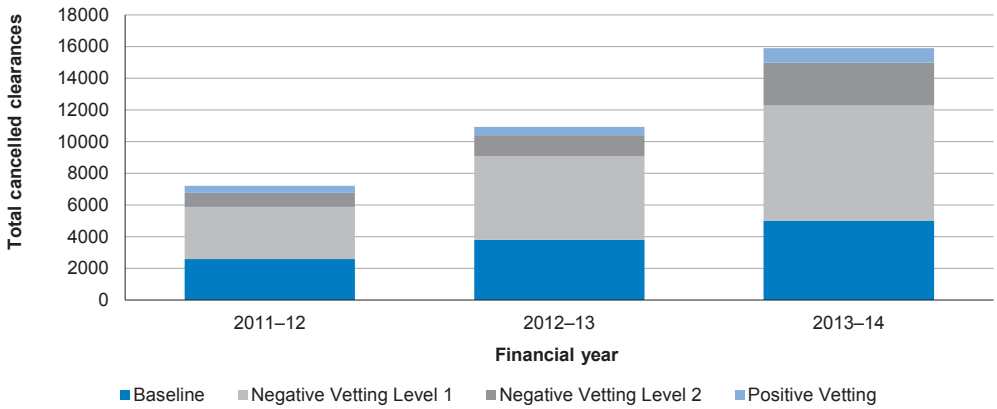
then makes a recommendation on the suitability of the individual to hold the clearance. On completion of the assessment, the AO submits a Vetting Analysis Report, which is then allocated to an AGSVA Delegate.[80]

Cancellation of clearance cases

3.14 In 2013–14, almost one-third of clearance cases were cancelled at some point during the vetting process. Cancellations occur when: the sponsoring entity cancels the clearance request; the clearance subject withdraws from the vetting process; or the clearance subject fails to provide required information within a specified timeframe. In some instances, AGSVA may expend a significant amount of effort before a case is cancelled.

3.15 Figure 3.2 shows the number of security clearance cases that were cancelled during the vetting process since AGSVA's first full year of operations. The data shows a steady increase in cancellations over time. AGSVA informed the ANAO that the increase is due to more complete records on cancelled cases, and more rigorous application of AGSVA's policy to cancel the clearance process when necessary information is not provided by the clearance subject within specified timeframes.

Figure 3.2: Number of security clearance cases cancelled during the vetting process, by level, 2011–2014



Source: Analysis of AGSVA annual reports to SCNS.

3.16 In the event that the sponsoring entity cancels the clearance request, AGSVA still charges a fee, which varies according to the timing of cancellation.

80 Delegates are also provided with all documentation relevant to the case to inform their decision.

While the fee is intended to recoup the cost of vetting work undertaken, the large number of cancellations is a drain on AGSVA's available resources. The underlying causes of cancellations require further attention to help identify opportunities for improved efficiency.

ASIO security assessments

3.17 The Australian Security Intelligence Organisation (ASIO) performs an integral role in processing NV1, NV2 and PV clearances, which require an ASIO security assessment as part of the minimum personnel checks (refer to Table 3.1).[81] AGSVA routinely provides ASIO with information collected during the course of the vetting assessment process to inform the ASIO security assessment. However, there has been a history of disagreement between AGSVA and ASIO about aspects of the process, such as when ASIO should commence the security assessment, and the amount and quality of information provided by AGSVA to ASIO. In response to a 2011–12 ANAO audit on security assessments of individuals[82], ASIO agreed to an ANAO recommendation to establish formal arrangements with its key customer entities, including AGSVA.[83] The formal arrangements were to address processing times for non-complex cases, the provision of updates on the status of complex cases and data quality expectations.

3.18 In early 2015, AGSVA and ASIO agreed that ASIO would commence its security assessment of individuals following the completion of AGSVA's vetting assessment.[84] This agreement means that ASIO has access to all the information collected during the vetting assessment process, and resolved one of the areas of disagreement between the two organisations. However, as at March 2015, a formal Protocol covering the full scope of AGSVA and ASIO interactions remained the subject of ongoing negotiations between AGSVA and ASIO. The finalisation of the formal arrangement would help clarify

81 ASIO's roles and responsibilities are set out in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act).

82 ANAO Audit Report, No.49, 2011–12, *Security Assessments of Individuals*, p. 30.

83 At the time of the 2011–12 ANAO audit, ASIO customer entities included: the then Department of Immigration and Citizenship; security vetting entities including AGSVA; and AusCheck.

84 Previously, AGSVA had requested that ASIO commence the security assessment at the same time as the AGSVA vetting assessment, when only basic information about the clearance subject was available.

mutual expectations and responsibilities, and contribute to both organisations fulfilling their role in the management of security vetting.[85]

Vetting decision

3.19 A Delegate is an AGSVA staff member appointed by Defence's Chief Security Officer to make decisions to grant or continue security clearances. The Delegate's role is to review the case and the recommendation made by the AO. The Delegate determines whether all necessary information has been provided, all relevant checks have been completed and whether to approve the AO recommendation, modify the recommendation or refer it back to the AO for re-work.

3.20 If a Delegate forms the view that a security clearance should be denied or revoked, the Delegate makes a recommendation and allocates the case to AGSVA's Complex Vetting Team (CVT). The CVT reviews the case and may request that further checks be conducted, before the final decision is made. The CVT aims to ensure that the final vetting decision is made in accordance with the PSPF and the principles of procedural fairness and natural justice.

Ongoing clearance maintenance

3.21 A security clearance represents an assessment of risk factors based on information provided by the clearance subject at the time of assessment. As a clearance holder's risk profile may change over time, ongoing review of a clearance holder's eligibility and suitability is required. Clearance maintenance is a responsibility shared by the clearance holder, the sponsoring entity and AGSVA. Clearance holders, sponsor entities or third parties may report relevant changes in personal circumstances to AGSVA. AGSVA responds to changes of circumstance, and conducts periodic reviews of security clearances and reviews for cause.[86]

3.22 The periodic review of security clearances is known as revalidation.[87] The process is intended to ascertain if the clearance holder continues to meet suitability requirements for their clearance level. Mandatory review periods for all security clearance levels were introduced with the release of the PSPF in June 2010 (Table 3.2).

---

85 Defence and ASIO informed the ANAO in May 2015 that the Protocol was expected to be signed in mid 2015.

86 Review for cause is a review which is triggered by a significant change in personal circumstances or a specific security concern.

87 Revalidation of PV clearances is also referred to as re-evaluation.

Table 3.2: Clearance review periods, introduced June 2010

Activity	Baseline	NV1	NV2	PV
Revalidation	15 years	10 years	5 years	5 years[a]

Source: AGSVA Policy and Procedure Document 2:8 Ongoing Clearance Management, 30 September 2014, p. 7; and AGD, *Australian Government Personnel Security Protocol*, Version 2.0, September 2014, p. 32.

Note a: PV clearance holders also undergo an annual security appraisal, which involves them completing a Security Appraisal Form and providing two referee reports.

3.23 AGSVA procedural documentation outlines the intended features of the periodic review process:

> The AGSVA will initiate all re-evaluations and revalidations. It is the responsibility of agencies to ensure their clearance holders comply with having their security clearances revalidated or re-evaluated within the [mandated] timeframes. There is a risk to agencies where a clearance holder does not complete the revalidation process. Without a revalidation, the AGSVA is not able to assess their continued suitability to hold a security clearance. If this occurs, the AGSVA will cancel the security clearance and notify both the agency and the clearance holder.[88]

Management of AGSVA's Industry Vetting Panel

3.24 AGSVA relies heavily on a contracted workforce to complete vetting assessments and supplement its APS staff. Chapter 1 described the three main types of contractors used by AGSVA.[89] The total number of contracted personnel used by AGSVA has increased over time (Table 3.3).

Table 3.3: Contracted personnel numbers over time

Contractor type	30 June 2011	30 June 2012	30 June 2013	30 June 2014
IVP	175	187	193	210
CareersMultiList	30	42	43	52
Psychology	47	46	47	48

Source: Data provided by AGSVA.

Note: Data does not include subcontractor personnel.

3.25 AGD's revised proposal to government in November 2009 to establish a centralised vetting unit within Defence noted that the majority of assessment work would be performed by Defence's APS staff. Defence's intention was to

88 Defence, AGSVA Governance, '1.0 Vetting Management System', 18 August 2014, p. 32.

89 Refer to paragraph 1.8.

use the IVP to augment internal capability and provide a surge capacity at times of high demand. However, AGSVA has relied on the IVP to complete a large proportion of vetting assessments. In 2013–14, over half of AGSVA's vetting assessments were allocated to the IVP, including approximately 90 per cent of cases at the NV1 and NV2 levels and 15 per cent at the PV level.[90] Defence's 2014 enterprise risk deep-dive analysis of AGSVA stated that 'while industry support panels were originally designed as a surge capacity, they form an integral part of the AGSVA's business-as-usual processes'.[91]

3.26 Users of contracted personnel should be confident that those personnel are acting in accordance with relevant policies and procedures. AGD's September 2014 Personnel Security Protocol states that 'Vetting agencies are to ensure contractors engaged in vetting meet the requirements of the PSPF and any agency specific policies or procedures.'[92]

3.27 The management of the IVP is formalised by Defence's Deed of Agreement for the Provision of Security Vetting Services (the Deed). AGSVA's Manager IVP oversees IVP vetting operations, the allocation of work to the IVP contractors, and IVP contractors' compliance with policies and procedures.[93] The Manager IVP also conducts an informal program of visits to IVP contractors to maintain contact and address specific concerns.

3.28 AGSVA Delegates review assessments and recommendations made by IVP AOs, and where the Delegate considers the work does not meet specified quality criteria, he or she identifies the case as a non-conforming product and refers it to the Manager IVP for remediation.[94] However, AGSVA's informal program of visits and review of vetting assessments does not provide adequate assurance as to whether IVP contractors comply fully with protective security policy requirements. In the absence of additional assurance measures, such as

90 Defence informed the ANAO that since August 2012, all Baseline clearance assessments have been completed by AGSVA's APS staff.

91 Defence, Deputy Secretary, Intelligence and Security, Defence Committee Agendum Paper, Enterprise Risk deep dive: Australian Government Security Vetting Agency, 17 February 2014, p. 4.

92 AGD, *Personnel Security Management Protocol*, Version 2.0, September 2014, p. 35.

93 IVP contractors are required to obtain and maintain membership of the Defence Industry Security Program (DISP) in accordance with the Deed. The DISP is a risk mitigation program managed by the Defence Security Authority which aims to ensure the Defence industry meets its security responsibilities. The DISP website states that 'All DISP members must comply with the security standards required by the Defence Security Manual (DSM), Australian Government Protective Security Manual (PSM) and Australian Government Information Security Manual (ISM)'.

94 The Director Quality Management measures and reports on the accuracy and timeliness of work completed by the IVP according to the number of cases returned for remediation.

an audit program, AGSVA relies on contractual obligations to promote IVP contractor adherence to protective security policy.

3.29 AGSVA's IVP Management Work Instruction noted that from 2014 AGSVA would conduct audits of each IVP company to 'provide assurance to [the Assistant Secretary Vetting] that the IVP companies have appropriate systems and processes in place to deliver a quality product – and that where concerns are identified, remediation measures are implemented.'[95] However, AGSVA has not yet conducted an audit of any of its IVP contractors. AGSVA's 2015 internal quality audit program notes that IVP audits will commence in the fourth quarter of 2015, with 25 per cent of contractors to be audited in 2015, another 50 per cent in 2016 and the remaining 25 per cent in 2017.

3.30 Implementation of the planned IVP audit program would strengthen assurance that IVP contractors have appropriate systems and processes, and adhere to policy requirements and relevant legislation.

Recommendation No.1

3.31 To provide additional assurance that AGSVA's Industry Vetting Panel (IVP) contractors are operating in accordance with applicable security policies and procedures, the ANAO recommends that Defence implement a targeted audit program to assess IVP contractors' operations.

Defence's response:

3.32 *Agreed.*

Compliance with protective security policy

3.33 AGVSA is required to conduct security vetting in accordance with Australian Government policy and guidelines. Sound vetting procedures and practices provide confidence to stakeholders that vetting is consistent and fair, and decisions are reliable. The ANAO reviewed:

- assessments of AGSVA's compliance with protective security policy since 2011;
- the qualifications of AGSVA staff and contractors; and

95 AGSVA, Business Administration, '4:7 Industry Vetting Panel Management', Version 1.1, 19 August 2014, pp. 15–16.

- AGSVA's quality internal audit program.

Assessments of compliance with protective security policy

3.34 There have been two key bodies of work to assess the compliance of AGSVA's procedures and systems with protective security policy. AGSVA engaged contractors to review its procedures and systems in 2012 and 2013; and three Defence internal audits undertaken in 2012, 2013 and 2014 also considered policy compliance.

3.35 In 2012, AGSVA engaged an external contractor to assess the compliance of its vetting procedures with the PSPF and Classified Protective Security Manual (CPSM). The contractor considered 146 requirements[96] and identified 63 gaps in AGSVA's procedures, leading to six major recommendations in the areas of: risk management; alignment with personnel security policy and guidelines; training; and oversight of the IVP.

3.36 In 2012–13, an external contractor assessed the compliance of AGSVA's procedures with the PSPF and supporting guidelines. The contractor's April 2013 report recorded no non-conformances but made over 200 observations, reflecting the incomplete status of AGSVA's documentation suite, which was still under development at that time.[97]

3.37 As previously discussed at paragraph 2.45, Recommendation No.3 of the IGIS report was that:

> The Defence Chief Audit Executive should review and report annually on AGSVA's compliance with all applicable Government security vetting policies, with the first review to be completed by 30 June 2012. The results of the reviews should be reported in Defence's annual report. The need for annual reviews should be reconsidered after three years.[98]

3.38 The findings of the internal audits conducted by the Defence Chief Audit Executive, as recommended in the IGIS report, are summarised in Table 3.4.

96 The scope of the audit included 24 criteria from the overarching PSPF document, 104 from the Personnel Security Protocol and 18 from the CPSM.

97 An 'observation' referred to a requirement which was partially addressed.

98 Inspector-General of Intelligence and Security, *Inquiry into Allegations of Inappropriate Vetting Practices in the Defence Security Authority and Related Matters*, 2011, p. 6.

Table 3.4: Defence internal audit findings on AGSVA's compliance with security vetting policy

Defence Internal Audit Report	Compliance with security vetting policy
June 2012	The internal audit report concluded that AGSVA was not fully compliant with security vetting policy. The report expressed confidence that implementation of the planned AGSVA Reform Agenda would result in full compliance.
August 2013	The internal audit assessed AGSVA's compliance against a sample of five security vetting policies. AGSVA was found to be compliant with the policies sampled.
September 2014	The internal audit concluded that AGSVA was compliant with personnel security policy PERSEC 5[99], and the supporting security vetting policies sampled as part of the audit. However, the audit also indicated that AGSVA was not compliant with the requirement for minimum competency levels for AOs and Delegates, an apparent contradiction of the more general finding.[a]

Source: Defence Audit and Fraud Control Division audit reports.

Note a: In relation to staff competency levels, AGSVA's policy was found to be consistent with government policy, but there was evidence that some AGSVA staff did not meet the competency requirements.

3.39 The 2014 Defence internal audit concluded that:

> Audit Branch has determined there is a need for further annual reviews of AGSVA however with a change in scope. The scope of the audit in its current format, with a predominant focus on IGIS recommendations and policy based compliance, is no longer required. The focus should be on ensuring the updated frameworks and quality management system developed are embedded in the AGSVA day-to-day operations and the AGSVA is operating efficiently and effectively.[100]

3.40 The Defence internal audits included limited independent testing of whether AGSVA's policies and procedures are applied correctly during the vetting process, and placed reliance on the compliance assessments of AGSVA's contractors in 2012 and 2013. There would be merit in future Defence internal audits substantively testing AGSVA's work practices against applicable Australian Government security policies and agreed vetting procedures for a sample of security clearances. This approach would provide a higher level of assurance that AGSVA's security vetting is performed in compliance with government policy.

---

99 At the time of the internal audit, PERSEC 5 which was the mandatory requirement in the PSPF stated: 'All Australian Government agencies must follow the Australian Government personnel security management protocol and supporting guidelines for personnel security.'

100 Defence, Defence Audit and Fraud Control Division, Audit Task: 14-003 'Australian Government Security Vetting Agency – Compliance with Security Vetting Policy', April 2014, p. 7.

AGSVA staff qualifications

3.41 The Personnel Security Vetting Practices Guidelines specify minimum qualifications for AOs:

> Assessing officers undertaking Positive Vetting, Negative Vetting Level 2 or complex vetting assessments are to hold a Certificate IV in Government Security (Personnel security stream) or equivalent.
>
> Assessing officers undertaking Negative Vetting Level 1 and Baseline Vetting assessments are to hold a Certificate III in Government Security (Personnel security stream) or equivalent.
>
> Vetting agencies are to regularly assess the competencies of all assessing officers and provide additional training and education to any officer with identified deficiencies.[101]

3.42 Ensuring the vetting workforce is adequately trained has proven difficult for AGSVA. The 2011 IGIS report found that AGSVA did not adequately train its APS staff and contractors. Further, in July 2013, an AGSVA internal quality audit found that training outcomes for Delegates were not appropriately recorded, and training documentation was inconsistent and uncontrolled.[102] The 2014 Defence internal audit noted that:

- not all security vetting staff within AGSVA hold mandatory security qualifications; and
- the development of ongoing training for security vetting staff has not been finalised.[103]

3.43 The ANAO requested documentation from AGSVA to confirm the Certificate IV qualifications of its APS AOs and Delegates. However, AGSVA provided inconsistent information from two different sources, and the data indicated that AGSVA had not sighted the qualifications of some AOs and Delegates. AGSVA's Director of Vetting Operations informed the ANAO in August 2014 that 'There are currently no staff in [the Directorate Vetting Operations] that do not hold a CERT IV or are not under appropriate training'.

---

101 Before the release of the *Vetting Practices Guidelines* in November 2014, the *Personnel Security Practitioners Guidelines* (2010) used the terminology 'should' rather than 'are to' in relation to personnel competency requirements.

102 Defence, Quality Internal Audit Programme, Process Audit, 'P6: Vetting Decision: Delegation', Final Internal Audit Report, 8 July 2013, p. 13.

103 Defence, Defence Audit and Fraud Control Division, Audit Task: 14-003, 'Australian Government Security Vetting Agency – Compliance with Security Vetting Policy', September 2014, p. 4.

However, the misalignment of records reviewed by the ANAO suggests that there is scope for AGSVA to improve its recordkeeping in relation to staff roles, qualifications and training.[104]

3.44 IVP AOs are also required to maintain minimum competency levels. This requirement is outlined in the Deed between AGSVA and the IVP contractors. AGSVA provided the ANAO with a 'Specified Personnel List' which is referred to in the Deed and intended to identify IVP AOs and their level of security vetting competency. However, AGSVA has not verified the stated competencies by sighting the relevant qualifications. As discussed, a program of IVP contractor audits would provide Defence with assurance that contracted requirements, including those relating to staff competencies, are being met.

AGSVA internal quality audit program

3.45 As discussed, AGSVA achieved ISO 9001 accreditation in April 2014. As part of this accreditation, AGSVA has implemented an internal quality audit program. AGSVA conducted 14 internal quality audits in 2013 covering the full range of AGSVA's activities carried out by APS staff. These audits revealed areas for improvement in every part of AGSVA's business. Some of the non-conformances and observations raised included:

- an inability to meet benchmark timeframes for vetting, which was unlikely to improve in the short to medium term;
- numerous and ongoing IT infrastructure problems, such as system downtime and network availability;
- variation in the extent of vetting checks applied during the delegation process;
- non-adherence to prescribed policies and procedures;
- inconsistent records management practices; and
- incorrect performance reporting.[105]

104 A draft AGSVA Quality Internal Audit report dated 22 August 2014 also found non-conformance in Records Management.

105 Defence, AGSVA Quality Internal Audit, Process Audit 'P2: Clearance Pre-assessment Coordination, Final Report', 22 July 2013, p. i.

3.46 AGSVA's 2014 internal quality audit program included eight process audits and four conformity audits, although only ten were completed.[106] Going forward, AGSVA needs to look beyond the milestone of gaining accreditation of its Quality Management System, and continue to support the internal quality audit function as a means to identify problems and promote continuous improvement.

Vetting assessments and decisions

3.47 The security vetting process is intended to determine whether an individual is suitable to hold a security clearance and access classified resources.[107] AOs and Delegates are responsible for making common sense recommendations and determinations on whether to grant clearances based on careful consideration of all available and reliable information, both favourable and unfavourable, about the clearance subject. Under the PSPF, 'Any doubt about the suitability of a clearance subject is to be resolved in favour of the National Interest.'[108]

3.48 The Personnel Security Vetting Practices Guidelines list seven 'factor areas' which are relevant in determining whether granting or continuing a clearance is consistent with the national interest.[109] For example, under the personal relationships and conduct factor area, association with persons involved in criminal activity would raise a security concern. The concern may be mitigated if the behaviour occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature.

3.49 AGSVA's vetting process (described at paragraphs 3.7 to 3.20) is intended to meet the minimum requirements of the Vetting Practices Guidelines and identify areas of security concern. It includes review of AO assessments, and aims to provide procedural fairness for individuals. Where security concerns are identified, the AO and Delegate may conduct additional

106 Several process audits were combined and five reports covering the eight process areas were completed during 2014. As at 12 January 2015, two conformity audits were completed but the reports had not been finalised, and two had not been conducted.

107 Appendix 3 outlines the factors considered when assessing an individual's suitability to hold a clearance.

108 AGD, *Protective Security Policy Framework*, Canberra, October 2014.

109 The seven factor areas are: external loyalties, influences and associations; personal relationships and conduct; financial considerations; alcohol and drug usage; criminal history and conduct; security attitudes and violations; and mental health disorders.

checks, and they are required to determine, on balance, whether there are mitigating factors or whether the issue constitutes a genuine security concern.

3.50 AGSVA processes around 50 000 clearance requests per year. Of these, up to 16 000 cases have been cancelled during the assessment process. The number of the remaining clearance requests which are not granted has been low (refer to Table 3.5). AGSVA informed the ANAO that the low rate of clearance denials is a result of:

- individuals having already been through a competitive selection process and completed pre-employment checks, resulting in a pool of clearance subjects who have been screened for eligibility and suitability for employment in government;
- individuals withdrawing from the vetting process and/or sponsoring entities cancelling cases when security concerns are identified (refer to Figure 3.2); and
- AGSVA's obligation to apply the principle of procedural fairness, which can result in mitigation of identified security concerns.[110]

Table 3.5: Number of clearances granted, denied or revoked

Financial year	Number of clearances granted	Number of clearances denied or revoked
October 2010 to June 2011	23 754	17
2011–12	39 323	8
2012–13	37 158	16
2013–14	33 255	21

Sources: AGSVA Annual Report to SCNS.

3.51 The low rate of clearance requests which are denied has raised a concern among some entities that security risks may not have been fully identified, or mitigated. This prompted several comments in response to the ANAO's September 2014 Questionnaire developed for this audit, including:

> We have had instances where a staff member who has been provided with an AGSVA clearance has had the same level of clearance rejected by, for example [another authorised vetting agency] when on secondment. Whilst the [authorised agency] may do their own or have access to more information, the

110 Procedural fairness is outlined in chapter 6 of the 2014 *Personnel Security Guidelines Vetting Practices*.

> findings in this instance raised a number of concerns within our agency as to how the same clearance was awarded by AGSVA.[111] …
>
> AGSVA have broadly devolved vetting practices and processes by employing a production-line ethos to all but the most sensitive clearances. This has been driven by efficiency, and there are concerns that important pieces of information are being overlooked or under-managed when a clearance is granted. Two cases within [the entity] have occurred in the last twelve months that support these concerns. …
>
> AGSVA have granted several clearances for [the entity] since its inception that have been contrary to the [Personnel Security Vetting Practices Guidelines] and proven questionable based on subsequent behaviours and incidents.

3.52 An AGSVA internal quality audit of the delegation function (July 2013) observed inconsistencies in the level of additional background checks required by different AOs and Delegates.[112] The audit found that some AOs and Delegates required additional checks and others did not for similar types of cases. This could result in unnecessary additional checks being conducted in some cases, which adds to the time taken to complete the vetting process. Conversely, insufficient checking by AOs could result in clearances being granted to individuals who may not be suitable. The differing approaches to risk adopted by some AOs and Delegates indicates that clearer guidance may be required.

3.53 The vetting decision by an AGSVA Delegate is the final quality gate for the majority of clearances.[113] However, there is currently no quality control framework for the final Delegate decision to grant or continue a clearance. During AGSVA's internal quality audit of the delegate function in 2013, Delegates suggested independent case sampling by peers be undertaken to help promote consistency and compliance with minimum standards. AGSVA's internal quality audit stated:

> AGSVA must determine whether it intends to monitor and measure Delegate output and how such monitoring and measurement could be applied. The essential non-conformance in this area at present is that there is no documented process in place and no decision about what and how to deal

111 ANAO comment: Defence informed the ANAO that while AGSVA conducts vetting in accordance with the PSPF, other authorised vetting agencies may incorporate additional agency specific checks that exceed the minimum PSPF requirements into their vetting process.

112 Many Delegates also perform the AO function. However, one individual cannot perform the AO and Delegate function for the same clearance.

113 Until revalidation (refer to Table 3.1).

with the issue of monitoring and measuring of the Vetting Decision: Delegation process.[114]

3.54 The development and implementation of a quality control framework would provide additional assurance regarding the quality and consistency of AGSVA's Delegate decisions. In particular, it would provide assurance to AGSVA's customers and stakeholders that the security clearance process meets the intent of national security policy. A mix of peer reviews as suggested by the internal quality audit, supplemented by periodic independent quality assurance, would be consistent with a better practice approach.

Recommendation No.2

3.55 To strengthen quality control over vetting decisions and promote consistent decision-making, the ANAO recommends that Defence introduce a program of internal peer review supplemented by periodic independent external quality assurance of Delegate decisions.

Defence's response:

3.56 *Agreed.*

Conclusion

3.57 Since 2012, AGSVA has introduced a revised management structure incorporating more appropriate governance arrangements, implemented a centrally managed suite of procedural documentation, and gained accreditation of its Quality Management System. AGSVA's security vetting process is well established and familiar to government entities that request clearances on a regular basis. However, in 2013–14, almost one-third of clearance cases were cancelled at some point during the vetting process, and the underlying causes of cancellations require further attention to help identify opportunities for improved efficiency. AGSVA should also improve the level of assurance over IVP contractors' work practices through a targeted audit program, and strengthen quality control over vetting decisions through a program of peer reviews and periodic independent quality assurance. These measures would help address inconsistencies in vetting assessment processes identified by AGSVA, and concerns raised by some stakeholders about the rigour of AGSVA's assessment process.

114 AGSVA, Quality Internal Audit Programme, Process Audit, 'P6: Vetting Decision: Delegation', 8 July 2013, p. 12.

4. Management of Information Systems

This chapter examines the development and management of AGSVA's information systems and security clearance data.

Introduction

4.1 AGSVA uses two primary information systems to process security clearances. The ePack[115] system allows clearance subjects to complete and submit their security vetting packs through an online portal, and the system uploads clearance information directly to PSAMS.[116] AGSVA uses PSAMS to capture security vetting information and manage vetting workflow. PSAMS interfaces with Defence's records management system, Objective, where the data is stored. AGSVA currently manages some 349 000 security clearances and is responsible for the security, availability and accuracy of sensitive clearance data.

4.2 In this chapter, the ANAO examines:

- recent upgrades of PSAMS and ePack;
- IVP contractor access to PSAMS; and
- AGSVA's management of security clearance data.

AGSVA's ICT system upgrades

4.3 In November 2006, the then Secretary of Defence directed that the Defence Security Authority (DSA) upgrade the technology used by the Defence Vetting Branch. In May 2008, Defence approved the PSAMS Refresh Project to upgrade the PSAMS and ePack systems. Defence expected to upgrade the ePack system by June 2009 and PSAMS by March 2010. The system upgrades had a combined original budget of $4.785 million.

115 Defence first released ePack in 2004 for personnel applying for a Defence security clearance.
116 Defence first released PSAMS in 1997.

Upgrade of the ePack system

4.4 Defence identified that a range of benefits would flow from the upgrade of ePack to ePack2, including:

- accessibility for anyone with a PC and an Internet connection;
- better data quality through a reduction in transcription errors;
- a reduction in the submission of incomplete security clearance packs;
- immediate entry of data into PSAMS; and
- automation of processes, supporting faster clearance throughput.

4.5 While Defence had planned to implement ePack2 by June 2009, this did not occur. The November 2009 decision to centralise security vetting within Defence, and the prospective changes in security clearance levels[117], further complicated the Refresh Project deliverables. The implementation of a version of ePack that could manage new whole-of-government clearance levels, interface with PSAMS and be accessed via the Internet became critical to the establishment of centralised vetting arrangements by 1 October 2010.

4.6 In April 2010, ePack2 underwent user acceptance testing against the ePack2 Test Strategy, which specified minimum exit criteria, including that 'There will be no outstanding Defects of Severity 1 or 2'.[118] However, the system failed user acceptance testing with 40 Severity 1 and 249 Severity 2 defects.[119] The test summary report noted that the minimum exit criteria 'have not been met' and that 'ePack 2 has not successfully passed [user acceptance testing] and therefore is not currently "Fit for Purpose".'[120]

4.7 On 14 September 2010, ePack2 was approved for production release, two weeks before AGSVA commenced operations. The Approval for

---

117 New national security clearance levels were introduced as part of the PSPF in July 2010.

118 The minimum ePack2 exit criteria included:
- Test cases/scenarios/scripts completed as per schedule;
- Expected results recorded and Defects raised where appropriate;
- Defects and/or issues investigated;
- There will be no outstanding defects of Severity 1 or 2;
- 98% of test cases/scenarios/scripts for the phase executed; and
- A mitigation plan and resolution timeframes, for any outstanding Severity 3, 4 or 5 Defects.

119 Outstanding defects totalled 704.

120 Defence, PSAMS Refresh – ePack2 Test Summary Report – 20100419 UAT Release, April 2010, p. 12.

Production Release noted that, as at 10 September 2010, there were 58 Severity 1 and 544 Severity 2 defects, which was significantly more than were detected in the testing conducted in April 2010.[121] The Approval for Production Release did not reference the ePack2 Test Strategy minimum exit criteria, instead stating that 'useability satisfied minimum requirements for DSA', although 'not all original ePack2 business requirements will be satisfied by the latest release candidate.' The focus was to ensure the system was available to all potential users, and could support the new security clearance levels.

4.8 In relation to the production release of ePack2 with a high rate of system errors, in 2011 the IGIS was advised that AGSVA:

> Had no real option other than to accept a less-than-perfect solution in September 2010 … [and] … could manage the inadequacies of ePack2 while they were being fixed.[122]

4.9 The release of ePack2 had significant implications for AGSVA's initial operations, particularly for the Client Service Centre (CSC). AGSVA staff informed the ANAO that the number of telephone calls to the CSC increased four-fold when AGSVA commenced operations, due mainly to clients experiencing difficulty with ePack2. Although ePack2 was released with a high number of critical errors, the increase in call volume had not been anticipated and the seven staff members at the CSC were overwhelmed by the calls for assistance. This problem was exacerbated by a lack of formal processes for managing ePack2 errors. For example, in 2011, the IGIS inquiry found that CSC staff had advised clearance subjects to submit incorrect information in an effort to work around known system errors in ePack2.[123]

4.10 Since 2010, Defence has completed a series of technical updates of ePack2. However, AGSVA's CSC staff informed the ANAO that ePack2 continues to experience useability, compatibility and stability issues. Common problems include an inability to save a partially completed clearance pack and return at a later time, and certain data formats not being accepted (for example, upper case, and spaces). These issues are reflected in feedback received by AGSVA from individuals who use the application, with one clearance subject commenting that ePack2 is 'riddled with system errors and loss of information.'

---

121 Active defects totalled 1508.

122 Inspector-General of Intelligence and Security, *Inquiry into allegations of inappropriate vetting practices in the Defence Security Authority and related matters*, December 2011, p. 43.

123 ibid., pp. 43–44.

Respondents to the ANAO's survey of government entities as part of this audit also identified ePack2 useability issues.[124] One entity commented in the 2014 Questionnaire that:

> This department continues to receive feedback on an ongoing basis from clearance subjects who find the [ePack2] difficult to use. One constant complaint is that clearance subjects are not able to advance through the pack; that is, if they are unable to respond to the current question, they cannot move forward to another question and come back later to provide the missing information. This means that completing the [ePack2] takes much longer than it otherwise would.

4.11 The ePack2 system is the public face of AGSVA, but remains a frustrating and difficult system for individual users to navigate. This raises efficiency and productivity issues for customer entities and the vetting process as a whole. Defence informed the ANAO in February 2015 that ePack2 remains subject to ongoing fixes and enhancements.

Upgrade of the PSAMS system

4.12 As mentioned in paragraph 4.3, Defence had planned to implement PSAMS2 by March 2010. The upgrade was expected to improve vetting workflow management and increase productivity throughout the vetting process. The Refresh Project also included delivery of improved reporting capability.

4.13 The decision to centralise vetting within Defence and changes to protective security policy meant the original PSAMS2 upgrade requirements had to be amended significantly. Additional requirements included the ability to: manage security clearances for other government entities; import entities' clearance data; and support revised security clearance levels. In February 2010, DSA requested that Defence's Chief Information Officer Group (CIOG) 're-scope and re-baseline' the PSAMS project plan to incorporate the new technical requirements. At that time, delivery of PSAMS2 was re-scheduled for February 2011. However, the delivery of PSAMS2 was again delayed on several occasions. Defence ultimately made the necessary changes to PSAMS to accommodate whole-of-government service delivery from October 2010, but did not implement PSAMS2 until December 2012.

---

124 The ANAO's September 2014 Questionnaire was addressed to entities and not individual clearance subjects. The majority of responses from entities were positive regarding ePack functionality. However, specific comments about ePack useability merit further exploration by AGSVA.

4.14 One of the key benefits expected of PSAMS2 was an improved controls environment. PSAMS2 workflow management functionality does not permit vetting personnel to progress through the vetting process without the completion of mandatory tasks. This requirement helps prevent the inappropriate vetting practices identified in the IGIS report. An April 2013 Compliance Assessment Report completed for AGSVA by an external contractor found 'A high level of compliance' in its assessment of PSAMS2 compliance against the PSPF, Personnel Security Protocol and guidelines.

4.15 Notwithstanding the improvements introduced by PSAMS2, there are a range of shortcomings in the system's functionality. In 2013, the PSAMS2 Post Implementation Gap Analysis Evaluation Report elaborated on the application's end-to-end capability:

> PSAMS2 causes delays to some activities within the vetting processes. Some vetting activities cannot be undertaken in the system and there are some which have become considerably more difficult in the system which contributes to staff frustrations, for example clearance maintenance functions.[125]

4.16 The ANAO observed that AGSVA's Aftercare Team[126] in Adelaide operate almost entirely outside PSAMS2 due to system limitations. The Aftercare Team instead manages its workflow using Microsoft Outlook to allocate and prioritise tasks. Further, PSAMS2 did not deliver the anticipated reporting functionality, which was ultimately provided under a separate project in September 2014.

4.17 As discussed at paragraph 2.54, Defence's Intelligence and Security Group (I&S) presented an analysis of AGSVA risks to the Defence Committee in February 2014. This analysis indicated that AGSVA's risk of performance failure was still very high and that 'These pressures have been exacerbated by ICT systems that have not yet delivered their intended workflow efficiencies.' I&S identified the need for long-term and potentially significant investment in ICT solutions because PSAMS2 does not have the 'functionality needed for the future'.[127]

---

125 Defence, PSAMS2 Post Implementation Gap Analysis Evaluation Report, September 2013, p. 6.

126 The Aftercare Team are responsible for a number of vetting functions including: managing changes of individuals' circumstances; recognising transfers of individuals between government entities; cancellations of clearances; and partner assessments.

127 Defence, Defence Committee (DC) Agendum Paper, Enterprise Risk deep dive: Australian Government Security Vetting Agency, 17 February 2014, p. 7.

Cost of PSAMS and ePack upgrades

4.18 The original budget to upgrade ePack and PSAMS was $4.785 million. AGSVA informed the ANAO that the final cost of the ICT upgrades was $5.627 million for ePack2 and $32.106 million for PSAMS2. The total cost of $37.733 million is almost eight times the original estimate. Defence documentation indicates that shortcomings in ICT project planning, insufficient application of ICT expertise, staff turnover and major changes in project scope to deliver whole-of-government vetting functionality requirements, contributed to the problems experienced by the ICT upgrades and the substantial cost increases.[128] Despite the additional expenditure, AGSVA's ICT systems continue to lack reliability and functionality.

Industry Vetting Panel access to the Personnel Security Assessment Management System

4.19 IVP contractors have a central role within AGSVA's business model. When a clearance request is allocated to an IVP contractor, the file is printed and delivered to the contractor by AGSVA. The contractor then conducts the assessment, completes a Vetting Analysis Report and returns all the documentation to AGSVA.

4.20 Reliance on manual processes at various stages creates significant logistical issues and delays for AGSVA, impacting its ability to meet benchmark timeframes and adding to operating costs. AGSVA expended over $1 million on freight and storage in 2013–14, and 14 staff were responsible for handling clearance packs assigned to IVP contractors. Defence's 2012 internal audit of AGSVA noted that the manual processes are inefficient, weaken the audit trail for security assessments and introduce a risk of human error.

4.21 PSAMS can be used to track the progress of security clearance cases which are assessed by APS staff, but this is not possible for cases which are assessed by IVP contractors. As a consequence, AGSVA has limited visibility of progress during the assessment process for the majority of NV clearances. This lack of visibility impedes AGSVA's ability to analyse the assessment process, identify potential improvements and implement more efficient practices.

---

128 In a similar vein, ANAO Audit Report No. 27 2014–15, *Electronic Health Records for Defence Personnel* identified major deficiencies in Defence's planning, budgeting and risk management for a new Defence electronic health system. The initial June 2009 project budget of $23.3 million increased almost five-fold to $133.3 million by February 2014.

4.22 When AGSVA commenced development of the upgraded PSAMS system in 2010, it was expected that manual processing issues relating to IVP contractors would be addressed. However, there have been ongoing delays in the provision of a technical solution, which is currently anticipated in 2016 at the earliest.

4.23 Contractor access to Defence ICT systems has also had implications for the provision of procedural information to the IVP contractors. IVP contractor representatives interviewed by the ANAO advised of a history of inconsistent advice and slow notification of procedural changes. More recently, procedural information has been made available to stakeholders on an AGSVA community site through govdex.[129] This represents a step towards improved communication with IVP contractors, with procedural information now available in one place.[130]

Management of security clearance data

4.24 When AGSVA commenced operations, clearance data previously held by government entities (except for other authorised vetting agencies) had to be transferred to AGSVA. As the Australian Government's primary security vetting unit, AGSVA continues to collect and retain a significant amount of sensitive information about security clearance holders.[131]

Transfer and accuracy of clearance data

4.25 As part of the implementation process for centralised vetting, clearance data held by other government entities was collected for incorporation into AGSVA's data repository, PSAMS. CIOG developed a process for transferring the data from other entities, including advice to entities on how to format the data for transfer. However, AGSVA encountered a range of problems which prevented automatic uploading of the data received from other entities. For example, some data was incompatible due to the use of a variety of date

129 The govdex service is hosted by the Department of Finance. It provides a secure online collaboration space for Australian government entities and supports information sharing and communications with stakeholders.

130 However, one IVP member informed the ANAO that little direction has been provided on how to use govdex. Others advised that govdex does not notify the user that a new document has been made available, or an amendment made. Other IVP contractors had not yet had sufficient time to assess the functionality of govdex and provide comment.

131 The ANAO did not systematically verify the integrity or security of AGSVA systems or data.

formats.[132] As a result, some of the clearance data was manually entered into PSAMS, and this was not completed until November 2014.[133]

4.26 In responding to the ANAO's September 2014 Questionnaire, some entities raised concerns about AGSVA's management of clearance data, and the accuracy and completeness of its records.[134] One entity stated that:

> AGSVA has consistently failed to rectify known data errors that were identified within the first year of its operation. This has resulted in literally thousands of this department's officers having [duplicate records] in PSAMS, some with incorrect and out-of-date data. The specific data involves the inversion of the individual's date and month of the grant of their clearance and more importantly, the inversion of the date and month of their date of birth. AGSVA's ongoing failure to rectify these known errors is in contradiction of Australian Privacy Principles 10 and 13.[135] This department has provided the AGSVA with correct and up-to-date data on more than one occasion since the errors were identified; to date, the AGSVA has failed to take action to address the errors and appears not to regard this as a priority.

4.27 The ANAO also identified a number of additional date-related anomalies in PSAMS2 data during the course of the audit. For example, the data indicated that:

- 268 clearance records were created by AGSVA on 1 January 2050;
- 60 clearance packs were received by AGSVA before 1992;
- eleven clearances were granted in the future (post 2038);
- one clearance was granted in 1884 and fell due for revalidation in 2034; and
- one clearance was created in 2008, with a revalidation date of 1982.

4.28 AGSVA informed the ANAO that data anomalies are rectified as they come to attention. However, there remains scope for a more proactive

132 PSAMS would only accept dates in the format DD/MM/YYYY.

133 In mid to late 2011, AGSVA analysed 75 623 external entity security clearance records for data quality. Of these records, 29 782 (39 per cent) could not be readily uploaded into PSAMS due to data quality issues.

134 In May 2014, AGSVA released an updated Security Officer Dashboard, which allows entities to conduct clearance subject searches, and check clearance data for specific individuals.

135 ANAO comment: The Australian Privacy Principles are contained in Schedule 1 of the *Privacy Amendment Act 2012*. Australian Privacy Principle 10 relates to quality of personal information. Principle 13 relates to correction of personal information. These Principles specify that entities must take reasonable steps to ensure that the personal information that the entity collects or holds is accurate, up-to-date and complete.

approach where anomalies can be readily identified, such as those listed in the previous paragraph, and where AGSVA is notified by clearance subjects or other government entities about data errors.

ICT user access controls

4.29 The Personnel Security Protocol specifies that entities are to limit access to, and dissemination of, Australian Government security classified resources to those personnel who need the resources to do their work. This is referred to as the 'need-to-know principle'.[136] The principle equally applies to AGSVA, which manages detailed records relating to approximately 349 000 active security clearances.

4.30 Information collected during the security vetting process is marked as 'Sensitive: Personal', and stored in Defence's records management system, Objective. Security clearance records contain a significant amount of sensitive personal information about individual clearance subjects.

4.31 The ANAO reviewed AGSVA's access control policies and procedures for Objective files, and found no formalised policy and inconsistent practices.[137] Further, the ANAO found instances of AGSVA staff having ICT system access which appeared to be in excess of that required. For example, two AGSVA staff members with no responsibility for vetting had access to a significant number of high-level clearance records. These records included whole-of-life personal information and assessments. When this was pointed out, those individuals indicated they were unaware they had such access, and did not consider that access to the information was necessary to perform their duties.

4.32 In late 2014 and early 2015, AGSVA conducted two reviews relating to the management of its information holdings. The reviews found that, in a number of areas, the management of security clearance data has not met Defence's risk management requirements for systems, and the requirements of the Australian Government Information Security Manual.

4.33 A November 2014 Information Management Review identified 91 risks relating to unauthorised access to and loss of information from AGSVA's information management systems, with 73 per cent of these risks assessed as

136 AGD, *Australian Government Personnel Security Protocol*, Version 2.0, Canberra, September 2014, pp. 4–5.

137 The ANAO assessed user access management in relation to: granting and revoking user access to the system, and staff commencements, terminations and movements.

High or Extreme. A February 2015 Threat and Risk Assessment (TRA) report on AGSVA's electronic vetting systems identified gaps in control mechanisms and instances of control breakdown relating to access to Personal Security Files and secure handling of sensitive information. The TRA report also found that PSAMS2 and ePack2 audit trails were inadequate, and actions identified in past TRA reports to treat unacceptably high risks to data security had not been implemented.

4.34 The identification of information management risks and issues is a step in the right direction for AGSVA, and an aid to improving its management of sensitive data. As discussed, a more proactive approach to addressing data anomalies is required. More broadly, disciplined management of data integrity and security is needed to effectively address the identified shortcomings in information management.

Conclusion

4.35 Defence has invested over $37 million since 2008 in upgrading AGSVA's core ICT systems and considered that the upgrades would make a marked difference to vetting performance. While ePack2 and PSAMS2 help ensure the completion of mandatory vetting tasks and compliance with policy requirements, the systems still lack reliability and functionality. Further, there is at times a reliance on inefficient hard copy documentation processes, and PSAMS2 does not support certain tasks performed by AGSVA as part of the ongoing management of clearances. Notwithstanding Defence's substantial investment in PSAMS2, the department formed the view in early 2014 that the system did not have the functionality needed for future vetting operations.

4.36 AGSVA currently manages some 349 000 security clearances and is responsible for the security, availability and accuracy of sensitive clearance data. The ANAO reviewed AGSVA's access control policies and procedures for Defence's records management system, and found no formalised policy and inconsistent practices, including instances where staff members could access a large number of high-level clearance records beyond their 'need to know'. A February 2015 Threat Risk Assessment (TRA) conducted by AGSVA on electronic vetting systems also identified issues relating to access controls and secure handling of sensitive information, and inadequate ePack and PSAMS audit trails. Defence needs to strengthen its controls framework for the management of sensitive personnel information captured as part of the security vetting process.

5. Performance Monitoring and Reporting

This chapter examines AGSVA's key performance indicators and performance reporting. It also examines the timeliness of AGSVA's security vetting services and entity feedback on the agency's performance.

Introduction

5.1 A sound monitoring and reporting regime supports the effective delivery of government services. Adequate performance information, particularly in relation to the efficiency and effectiveness of service delivery, enables entities to assess their performance, adjust management approaches as required, and transparently report service delivery outcomes to stakeholders.

5.2 As the Australian Government's primary security vetting agency, AGSVA is expected to provide an effective service that enables government entities to confidently deploy personnel to perform sensitive work using security classified resources. AGSVA is also expected to provide an efficient service that enables entities to deploy personnel in a timely way.

5.3 In this chapter, the ANAO examines:

- AGSVA's performance monitoring and reporting framework, including key performance indicators (KPIs);
- the timeliness of security vetting services;
- AGSVA's budget and expenditure between 2010–11 and 2013–14; and
- entity feedback on AGSVA's performance.

Performance monitoring and reporting framework

5.4 The ANAO examined Defence's Portfolio Budget Statements (PBS) and the AGSVA *Service Level Charter* (Charter) to determine the extent to which these elements contributed to a sound performance monitoring and reporting framework for AGSVA.

5.5 Entities are required to establish deliverables and KPIs for each program in the PBS. Deliverables represent the goods and services produced and delivered by the program in meeting its objectives. KPIs provide

qualitative or quantitative information on the effectiveness of programs in achieving their objectives, in support of intended government outcomes.

5.6 AGSVA forms part of Defence's Program 1.5 – Intelligence Capabilities in the 2014–15 PBS.[138] Program 1.5 includes two deliverables which specifically relate to AGSVA:

- Meet the Australian Government Security Vetting Agency's key performance results as specified in the Charter.
- Strengthen the Management Framework of the Australian Government Security Vetting Agency.[139]

5.7 AGSVA's KPIs are set out in its Charter. AGSVA's four KPIs identify the performance levels AGSVA is expected to achieve in relation to the range of vetting services it provides (Table 5.1).

Table 5.1: AGSVA key performance indicators

KPI	Description[a]
1.	Meet clearance benchmark timeframes for 95 per cent of cases.
2.	Make Defence Internet system available to accept ePacks more than 99 per cent of the time, excluding scheduled and notified outages.
3.	Action all calls to AGSVA Customer Relationship Managers or the Customer Service Centre between 8:30 and 17:00 (Australian Eastern Standard Time) within 30 minutes.
4.	Provide all agencies with a monthly update on the status of all clearances that are not completed within the benchmark time.

Source: Department of Defence, *AGSVA Service Level Charter*, July 2014.

Note a: The same KPIs were included in the original AGSVA charter of 2010.

5.8 In relation to the completion of 95 per cent of clearance cases within benchmark timeframes, the minutes of the August 2011 AGSVA Better Regulation Ministerial Partnership (BRMP) Steering Committee included that:

> … at least ten per cent of all cases are complex, requiring additional time and effort to finalise. With this in mind, the AGSVA considers the existing KPI requirement to complete 95 per cent of clearance cases within benchmark completion time to be unachievable; a KPI of 90 per cent was proposed. The

138 Budgeting occurs at the program level in the PBS. As an activity within a program, Defence does not publicly report the budget for the security vetting services provided by AGSVA.

139 Defence, Portfolio Budget Statements 2014–15, p. 44.

committee concluded that customer agencies would be unlikely to welcome a reduction in the KPI as proposed.[140]

5.9 The Charter also outlines the benchmark timeframes to be met by AGSVA (Table 5.2). Measurement of the time taken by AGSVA to process a security clearance commences when the agency receives a complete vetting pack including supporting documentation, and finishes when a clearance determination has been made by AGSVA. The Charter states that:

> AGSVA aims to finalise clearances within benchmark times and is committed to completing them faster if possible, subject to not undermining the standard vetting processes and PSPF compliance, and timely support from external agencies.[141]

Table 5.2: Benchmark timeframes for security clearance completion

Clearance level	Benchmark processing time[a]
Baseline	One month
NV1	Four months
NV2	Six months
PV	Six months

Source: Department of Defence, *AGSVA Service Level Charter*, July 2014.

Note a: The same benchmark times were included in the original AGSVA Charter of 2010.

Assessment of key performance indicators

5.10 In 2012–13, the ANAO developed a set of three criteria to evaluate the appropriateness of entity KPIs. The criteria consider whether KPIs are relevant (focused and understandable), reliable (measurable and free from bias) and complete (balanced and collective).[142] The ANAO reviewed AGSVA's KPIs against the criteria.

5.11 Overall, AGSVA's KPIs do not represent a complete set of measures that collectively provide a balanced perspective on performance. While the first KPI on benchmark timeframes is a relevant measure of AGSVA's

140 Defence, minutes of 18 August 2011 meeting of the Australian Government Security Vetting Agency (AGSVA) Better Regulation Ministerial Partnership (BRMP) Steering Committee, 11 November 2011.

141 Defence, *AGSVA Service Level Charter*, July 2014, p. 3.

142 See ANAO Audit Report No.28 2012–13, *The Australian Government Performance Measurement and Reporting Framework*, p. 63.

efficiency in meeting customer demand, the remaining KPIs are not useful in assessing the effectiveness of AGSVA's delivery of vetting services:

- KPI 2 addresses the availability of the online ePack application but not client satisfaction with the application, which is a key measure of effectiveness from the client perspective.[143]
- While KPI 3 requires that all calls to the AGSVA Customer Relationship Managers or Customer Service Centre are actioned within 30 minutes, the term 'action' is not adequately defined, and as a consequence the KPI is not readily measurable.[144] [145]
- KPI 4 is to provide a status update to entities on clearances, which is an administrative process, rather than a direct measure of AGSVA's performance in delivering security vetting services.

5.12 Consideration should be given to incorporating a revised set of KPIs, including measures of both the efficiency and effectiveness of AGSVA's service delivery, in the Charter. This approach would be consistent with AGSVA's role as the primary provider of vetting services for the Australian Government, and would involve AGSVA obtaining feedback from government entities and clearance subjects about service delivery.

External reporting on performance

5.13 The Defence PBS and AGSVA's Charter provide for external reporting on AGSVA's performance. Reporting against the relevant PBS deliverables in the Defence Annual Report is intended to inform stakeholders about AGSVA's performance. The Charter requires that AGSVA: report monthly to government entities on the processing of security clearances; report annually to

143 Four entities raised concerns about ePack useability in response to the ANAO's September 2014 Questionnaire.

144 In December 2013, KPI 3 was identified as problematic in an AGSVA internal quality audit report. The report stated that KPI 3:

> is not adequately defined making it of limited utility and difficult, if not impossible, to accurately report against. The term "*action*" within the KPI statement requires definition.

Defence, AGSVA Quality Internal Audit Programme: Conformity Audit C4: Product Realisation, December 2013, pp. 3–8.

145 A more appropriate client service KPI would indicate a timeframe for completion of specified action. For example 'finalise query to the client's satisfaction'. Alternatively, it could incorporate a level of satisfaction with data gathered through regular surveys.

the Secretaries' Committee on National Security (SCNS)[146]; and publish a statement of its performance against the Charter on the AGSVA website.

Annual Report

5.14 The Defence Annual Report is the primary reporting mechanism to inform the Parliament and public about AGSVA's performance. The Defence Annual Report has included an assessment of AGSVA's performance against the relevant Defence PBS Program 1.5 deliverables (refer to paragraph 5.6). Until 2012–13, Defence used a system of up to three ticks[147] to indicate its assessment of the level of performance against a particular deliverable, referred to as 'status', and incorporated comments against those deliverables. In June 2013, the Joint Standing Committee on Foreign Affairs, Defence and Trade commented that:

> The three tick system is an exceptionally crude performance measurement methodology … It is not clear what the performance targets are, how they are devised, or how performance is assessed … it is very difficult to track defence performance over time in any meaningful way.[148]

5.15 In 2012–13, Defence moved to a system of four statements to indicate performance against deliverables: met, substantially met, partially met, or not met (refer to Table 5.3).

146 SCNS is the senior inter-departmental committee supporting the National Security Committee of the Cabinet (NSC). The committee is chaired by the Secretary of the Department of the Prime Minister and Cabinet. It considers all matters to be put before the NSC with a view to maintaining coordinated policy on national security.

147 One tick (✓) indicated the target was partially achieved, two ticks (✓✓) indicated the target was substantially achieved, and three ticks (✓✓✓) indicated all targets were met or exceeded.

148 The Defence Sub-Committee of the Joint Standing Committee on Foreign Affairs, Defence and Trade *Review of the Defence Annual Report 2011–12,* June 2013, p. 82.

Table 5.3: AGSVA performance reporting in Defence Annual Reports

Deliverable	Comments against deliverable	Status
2009–10		
Streamline the personnel vetting process.	The Defence Security Agency has improved the personnel vetting process and reduced the backlog of security clearances. A technology-enabled vetting system is scheduled for delivery in late 2010 to meet the requirements of the Australian Government Security Vetting Agency.	✓✓✓
2010–11		
Establish the Australian Government Security Vetting Agency.	The Australian Government Security Vetting Agency has yet to meet all of its KPIs, in particular [those] that relate to the number of clearances completed within benchmark times. Following allegations of inappropriate vetting practices in 2009–10, work is underway to confirm that all vetting processes are documented and endorsed and that the Information Technology systems supporting the vetting process are functional and allow data transfer as required.	✓
2011–12		
Meet the AGSVA's key performance results as specified in the agency's Service Level Charter.	The AGSVA met three of the four KPIs specified in the AGSVA Service Level Charter. It failed to meet KPI 1 – Meet Clearance Benchmarks in 95 per cent of cases, largely due to the resources being diverted to implement the AGSVA's significant reform agenda and remediation work in response to the Inspector General of Intelligence and Security recommendations.	✓
2012–13		
Meet the AGSVA's key performance results as specified in the agency's Service Level Charter.[a]	Due to reform activities and systems transition, the AGSVA consistently met only one (availability of the ePack system) of the four key performance indicators specified in its Service Level Charter.	Partially met
2013–14		
Meet the AGSVA's key performance results as specified in the agency's Service Level Charter.[a]	The agency met three of the four key performance indicators. The agency did not meet 45 per cent of KPI 1 – 'meet clearance benchmarks in 95 per cent of cases' – largely due to reform activities and problematic incorporation of a new ICT system.	Partially met

Source: Department of Defence, *Defence Annual Reports*, 2009–10 to 2013–14.

Note a: Defence also reported that it substantially met the deliverable 'strengthen the management framework of the Australian Government Security Vetting Agency'.

5.16 The reporting on AGSVA in the Defence Annual Report has been opaque and has not provided meaningful insights into AGSVA's performance. The KPIs used to assess AGSVA's performance have not been clearly specified,

and readers have to refer to the separate Charter to understand the full set of KPIs. The reporting on AGSVA's performance against its KPI's has also been very limited. The *Defence Annual Report 2013–14* included for the first time the proportion of security clearances completed in timeframes exceeding the benchmarks (45 per cent of cases).

5.17 There would be benefit in Defence incorporating KPIs addressing the efficiency and effectiveness of AGSVA's service delivery (refer to paragraph 5.12) in the deliverable column of its Annual Report, and providing a clear assessment of performance against each of those KPIs in the comments column. This would strengthen accountability for performance, provide more meaningful information to stakeholders and allow assessment of performance over time. This approach is particularly relevant for the delivery of a whole-of-government service by a monopoly provider, the performance of which can directly affect the operations of other government entities.

Reporting on complaints in the Defence Annual Report

5.18 Government requirements for departmental Annual Reports provide that:

> For departments which are required to have **service charters** in place, reference to performance against the service charter customer service standards, complaints data, trend analysis, and the department's general response to complaints must also be included.[149]

5.19 In relation to this requirement, in mid-2013, AGSVA implemented a feedback register to record customer feedback, complaints and suggestions. The register was provided to the ANAO in September 2014 and at that time contained 174 entries, including 65 which were recorded as complaints.[150] However, Defence has not reported complaints data in any Annual Report.

Other performance reporting

5.20 As required by the Charter (refer to paragraph 5.13), AGSVA has reported monthly to government entities on the processing of security clearances. Ninety-one per cent of the entities that responded to the ANAO's September 2014 Questionnaire agreed that the reports were useful. Several suggested there was scope for additional information to be provided, such as

149 Department of the Prime Minister and Cabinet, *Requirements for Annual Reports For Departments, Executive Agencies and FMA Act Bodies*, May 2014, p. 8.

150 139 of the entries had been closed.

the status of complex cases, reviews for cause and revalidations. More generally, only 52 per cent of the survey respondents agreed that AGSVA communicates effectively about the status of security clearances.

5.21 AGSVA's annual reports to SCNS have provided clearance processing data and a brief assessment of AGSVA's level of performance against its KPIs. The reports have also included details of: revenue received by AGSVA through clearance fees; activities which have occurred in the preceding year, such as reviews, audits and business reforms; and any proposed changes to the Charter.

5.22 While the Charter states that AGSVA will publish a statement of performance against the Charter on its website, as at December 2014, AGSVA had not published any performance information on its website, against either the 2010 or any subsequent Charter.

Timeliness of security vetting services

5.23 The timeliness of AGSVA's security vetting services can have a direct impact on the capability of government entities. For example, delays in the vetting process may result in job candidates taking up positions with other organisations, and entities may not be able to deploy personnel to conduct sensitive work in a timely manner. The ANAO reviewed the timeliness of AGSVA's security vetting services against the agreed benchmark timeframes for completion of clearances (Table 5.2).

5.24 By way of background, in July 2008, in response to the AGD Scoping Study on decentralised vetting activity, Defence reported clearance completion times ranging from 55.5 to 142 working days against the clearance levels which were active at that time. Internal Defence reporting and reviews had repeatedly identified issues with meeting clearance demand and a history of backlogs.

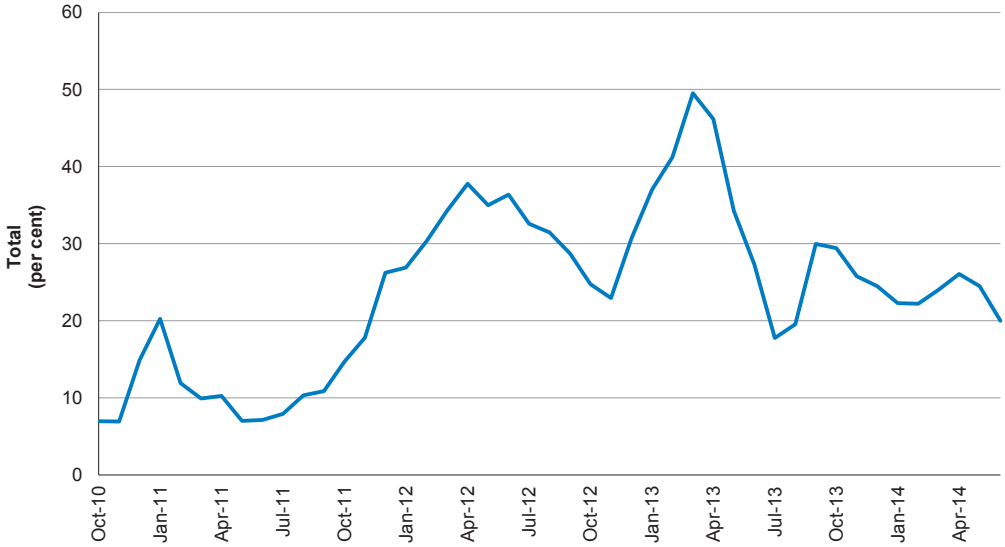
5.25 Under the Charter, the agreed Benchmark timeframes for completion of clearances range from one month (approximately 20 working days) to six months (approximately 120 working days), depending on the clearance level, and AGSVA aims to finalise 95 per cent of clearances within these timeframes.[151] The benchmark timeframes are challenging given the history of

151 The ANAO approached Defence, AGD and the Department of Finance to ascertain the basis for the benchmark timeframes and the 95 per cent ratio. Departments were unable to identify the rationale behind these performance targets.

clearance processing within Defence, and whole-of-government service delivery requirements.

5.26 The ANAO reviewed AGSVA's performance against the benchmark timeframes. Figure 5.1 shows the reported percentage of security clearance cases in progress for longer than the relevant benchmark timeframe (that is, overdue), between October 2010 and June 2014. From late-2011, AGSVA's performance deteriorated and the agency has not come close to meeting its target of finalising 95 per cent of clearances within the benchmark timeframes since that time. By mid-2014, around 20 per cent of clearances were overdue for completion, and there was no discernible improvement in AGSVA's processing performance during 2013–14.[152]

Figure 5.1: Percentage of cases in progress for longer than the relevant benchmark, October 2010 to June 2014



Source: Analysis of AGSVA annual reports to SCNS over multiple years.

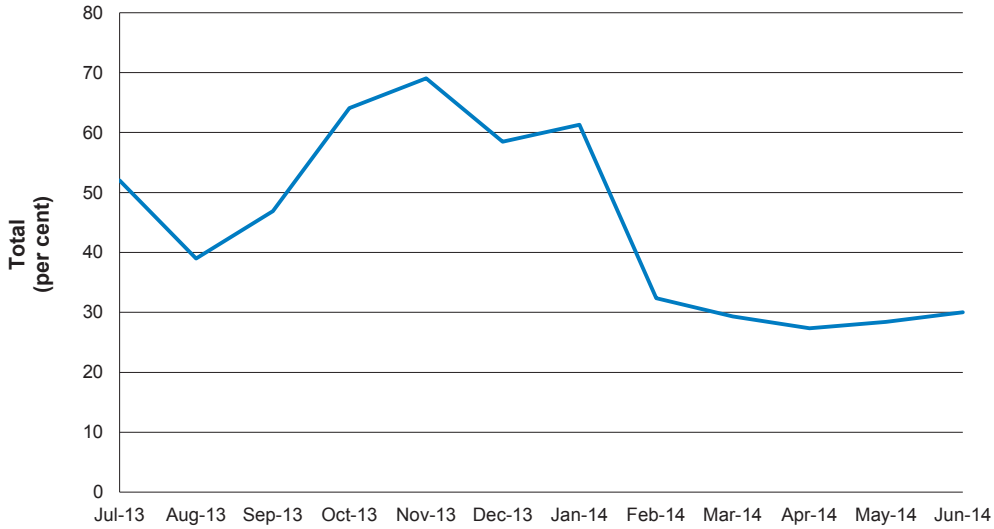
Note: The figure includes data for all clearance levels.

5.27 With the introduction of PSAMS2 in December 2012, AGSVA was able to report on the number of cases completed which exceeded benchmark

152 The increase in clearances in progress for longer than the relevant benchmarks between January and April 2013 coincided with the introduction of PSAMS2 and the problems associated with its introduction, which affected productivity.

timeframes.[153] Figure 5.2 shows the reported percentage of cases completed in timeframes exceeding the relevant benchmark during 2013–14. By mid-2014, around 30 per cent of security clearance cases were being completed in timeframes that exceeded AGSVA's benchmarks, as compared to the five per cent target.

Figure 5.2: Percentage of cases completed in a timeframe longer than the relevant benchmark, 2013–14



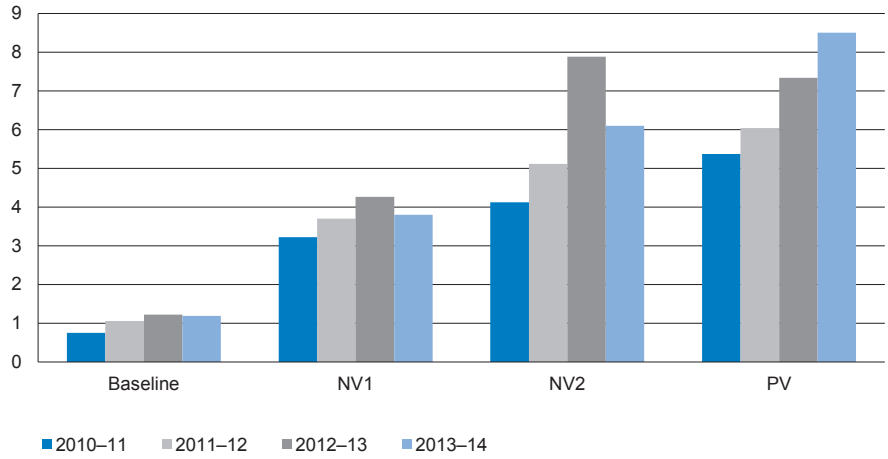
Source: Analysis of AGSVA's 2013–14 annual report to SCNS.

Note: The figure includes data for all clearance levels.

5.28 Figure 5.3 shows the reported average time taken to complete security clearances, for each clearance level. The reported average processing times for Baseline and NV1 clearances have been slightly above or below the respective benchmark timeframe. The reported average processing time for NV2 clearances was below the six month benchmark timeframe in 2010–11 and 2011–12, significantly above the benchmark in 2012–13, and close to the benchmark in 2013–14. The reported average processing time for PV clearances has been rising steadily since 2010–11, and exceeded the six month benchmark by around 40 per cent in 2013–14.

153 The ANAO sought to verify AGSVA's reporting using PSAMS2 data, and was able to broadly replicate the results.

Figure 5.3: Average processing times in months, by clearance level



Source: ANAO analysis of AGSVA annual reports to SCNS 2010–11 to 2013–14.

Note: Benchmark timeframes are: Baseline – one month; NV1 – four months; NV2 – six months; and PV – six months.

Revalidation backlogs

5.29 Several high profile international incidents have highlighted the 'insider threat'[154] faced by governments worldwide, particularly as a result of increasing reliance on information and communications technology (ICT). A key risk mitigation measure is the periodic review of security clearances to assess each individual's ongoing suitability to hold a clearance. In the Australian Government context, clearances are to be revalidated at set intervals (refer to Table 3.2 on page 68).

5.30 In a July 2014 AGSVA agendum paper, AGSVA reported approximately 10 700 security clearances as overdue for revalidation.[155] As at 30 March 2015, PSAMS2 data indicated that 13 175 clearances at the current levels were overdue

154 The insider threat is defined by AGD as the threat posed by unauthorised access, use or disclosure of privileged information, techniques, technology, assets or premises by an individual with legitimate or indirect access, which may cause harm. One prominent example of unauthorised activity is Edward Snowden, a former United States Central Intelligence Agency employee and National Security Agency (NSA) contractor who removed up to 1.8 million classified documents from the NSA. AGD, *Managing the Insider Threat to your Business*, 2014 p. 2.

155 Defence, AGSVA Stakeholder Engagement Forum, Agendum Paper 7/14 – *Revalidation Strategy Update*, 18 July 2014, p. 1.

Defence informed the ANAO that this figure did not include an estimated 2589 revalidation cases which were in progress at that time but not completed. However, the ANAO was not in a position to assess the figure due to limitations in Defence's data.

for revalidation.[156] In 2013–14, AGSVA reported that it completed 2597 revalidations, and cancelled another 2649 clearances during the revalidation process. The backlog of revalidations is a consequence of AGSVA using available resources to prioritise processing initial clearances, so as to enable employees and contractors to start work in positions that require a security clearance.

5.31 In order to address this backlog, AGSVA has recently initiated the review process for a large number of clearances. As at 30 March 2015, around 10 000 revalidation cases had been initiated, and almost 5000 completed clearance packs had been received and were being processed by AGSVA. While this represents a significant effort to deal with the backlog of clearances overdue for review, it also creates a substantial additional workload for AGSVA, which may lead to longer timeframes for processing initial clearances in the absence of additional vetting resources.

5.32 A PV clearance is the highest security clearance an individual can be granted, allowing the holder to access classified resources at all levels, and it is therefore particularly important to ensure that PV clearances are revalidated on time. In a July 2014 AGSVA agendum paper, AGSVA reported that 1402 PV clearances were overdue for revalidation.[157] As at 30 March 2015, PSAMS2 data indicated that the number of overdue PV clearances had increased to 3173. AGSVA reported it completed 420 revalidations of PV clearances in 2013–14[158], with 85 per cent of the cases taking longer than the benchmark timeframe of six months to complete.

Revalidation of clearances issued at the previous levels

5.33 When AGSVA was established, the agency assumed responsibility for clearances granted under the previous decentralised vetting arrangements, including Restricted, Confidential and Protected clearances (refer to Table 1.2). The enterprise risk deep-dive analysis of AGSVA that was presented to the Defence Committee in February 2014 noted:

> … there is in excess of 16,000 clearances at the previous levels of Restricted, Confidential and Protected that were issued prior to late 1998 that may be due

156 This figure includes revalidation cases in progress but not completed.

157 Defence, AGSVA Stakeholder Engagement Forum, Agendum Paper 7/14 – *Revalidation Strategy Update*, 18 July 2014, p. 1.
Defence informed the ANAO that this figure did not include an estimated 417 PV revalidation cases which were in progress at that time but not completed. However, the ANAO was not in a position to assess the figure due to limitations in Defence's data.

158 A further 491 PV revalidation cases were cancelled during the vetting process.

> for revalidation action. Government is yet to make a policy decision on their equivalent security clearance level under the new Australian Government Security Clearance System, but these clearances are in excess of fifteen years old.[159] [160]

5.34 AGSVA's report to the Defence Force Structure Review in May 2014 stated that there were 'almost 40 000 Confidential and Restricted clearances (primarily Defence) which will need examination.'[161]

5.35 The number of security clearances granted under the former classification regime that are overdue for revalidation may be significantly higher than reported by Defence. ANAO analysis of PSAMS2 data in December 2014 identified that 147 927 'active' clearances were recorded at the previous security clearance levels. For 115 000 of these clearances, Defence had recorded a revalidation date 50 years after the date the clearance was granted. This could result in the clearances being excluded from the periodic review process.

5.36 In June 2014, AGSVA explained in an internal brief that:

> Confidential level and below clearances will be dealt with in the longer term due to their lower risk to the Commonwealth than those clearances at the Negative Vetting Level 1 and above.[162]

5.37 The circumstances and behaviours of individuals change over time, and AGSVA and sponsoring entities need to be confident of individuals' ongoing suitability to hold a clearance at the relevant level. A realistic approach is required to quantify and deal with the backlog of revalidation work, including clearances granted at the previous levels.

5.38 The preceding paragraphs highlight AGSVA's longstanding inability to meet agreed performance targets for processing security clearance requests and to manage revalidations within agreed timeframes. Defence should develop a pathway—including agreed strategies, targeted resources and a timetable—to improve its performance against benchmark timeframes, and

---

159 Defence, Defence Committee (DC) Agendum Paper, Enterprise Risk deep dive: Australian Government Security Vetting Agency, Attachment A2, 17 February 2014, p. 2.

160 In June 2015, Defence advised the ANAO that the figure was calculated on the basis of a 10 year revalidation timeframe and excluded clearances that had the revalidation date changed as part of the PSAMS2 implementation.

161 In June 2015, Defence advised the ANAO that the figure was calculated on the basis of a 15 year revalidation timeframe and included all clearances that had the revalidation date changed as part of the PSAMS2 implementation.

162 Defence, Brief for A/ASV, Australian Government Security Vetting Agency Revalidation Strategy Update, 5 June 2014, p. 3.

address the revalidation backlog at a time of heightened focus on the threat posed by trusted insiders.

Recommendation No.3

5.39 To improve efficiency and maintain the integrity of security vetting, the ANAO recommends that Defence develop a clear pathway to achieve agreed timeframes for processing and revalidating security clearances.

Defence's response:

5.40 *Agreed.*

Capacity to deliver security vetting services

5.41 Persistent shortcomings in the timeliness of AGSVA's security clearance processing indicate that there are constraints in the agency's capacity to manage its workload. In 2013, an external review of AGSVA's business model and resourcing indicated that:

> From its inception AGSVA has struggled to manage the volume of work. Since December 2010 through to November 2013 it has failed to meet its key performance indicator for clearance completion times in every month. … AGSVA has managed to contain the backlogs for new clearances by deferring revalidations and re-evaluations.[163]

5.42 A May 2014 AGSVA submission to the Defence Force Structure Review advised that the agency 'remains unable to meet its key performance targets or adequately address a growing backlog of security clearance revalidations.' AGSVA cited a 'capability gap' caused by inadequate resourcing as the main cause of its inability to meet agreed performance targets. This is exacerbated by an ICT capability (PSAMS2) which has not delivered expected efficiencies despite four years of work and expenditure of over $32 million. Further, there is at times a reliance on inefficient hard copy documentation processes. While the IVP has additional capacity, allocating more work to the IVP comes at a cost and would require additional personnel to manually handle vetting data transferred to and from contractors.[164]

---

163 Remote, AGSVA Resourcing 2014–15 Review, 2013, p. 2.

164 The AGSVA submission to the Defence Force Structure Review in May 2014 stated:

> the IVP have a capacity of 4750 cases per month and are being allocated approximately 1870 cases per month, however due to the manual process of allocating cases to the IVP there is a limit to how many can be physically allocated.

Factors which influence demand for security clearances

5.43 AGSVA's ability to meet agreed benchmark timeframes for processing security clearances is dependent on the level of entity demand for vetting services. Concerns were raised in the media during 2014 that government entities at times require security clearances for positions that do not involve sensitive work, and that these practices unnecessarily increase demand for vetting and the associated cost to government. For example:

> The Industry Department in Canberra is hiring a plumber, who will need a clearance. The Plague Locust Commission wants two junior staff (APS level 2 officers) for field work in country NSW and Queensland. They, too, must be vetted.[165]

5.44 Entities may require staff or contractors to hold a security clearance for a variety of reasons. For example, to enable access to security classified resources, or to provide a level of assurance as to an individual's suitability to perform particular roles. Further, many government entities' records management systems are classified at the Protected level, necessitating all employees to hold a Baseline clearance.

5.45 Of the 23 entities that responded to the ANAO's September 2014 Questionnaire, six required a Baseline security clearance as a minimum to enable access to Protected level networks. Another two entities imposed security clearance requirements according to position levels. For example, one entity required all Senor Executive Service officers to hold an NV2 clearance. The remaining 15 entities informed the ANAO that they managed security clearance requirements according to the need for access to classified information.

Budget and expenditure

5.46 The establishment of a centralised vetting unit was expected to result in whole-of-government savings of $5.3 million per year. Table 5.4 shows reported operating expenditure incurred by AGSVA for each complete financial year since its establishment. It also shows estimated centralised vetting unit costs at the time of AGD's proposal in November 2009. Overall, reported operating expenditure for 2011–12 to 2013–14 was some 21 per cent higher than anticipated in November 2009. The additional expenditure has been funded from within

165 Marcus Mannheim, 'Secret state: costly government security clearances 'spiralling out of control', *The Sydney Morning Herald*, 23 June 2014.

Defence's overall budget, eroding the savings anticipated from centralised vetting.

Table 5.4: AGSVA operating expenditure ($m)

Description	2011–12	2012–13	2013–14
Personnel	20.258	22.305	23.578
Suppliers	23.318	28.130	21.548
Rental expenditure	1.428	0.875	0.926
Other		2.716	3.006
Total expenditure	45.004	54.026	49.058
Estimated expenditure	39.515	40.751	42.141

Source: Expenditure data provided by Defence; and AGD's November 2009 proposal.

Note: The reported operating expenditure does not include expenditure to upgrade ePack and PSAMS, which amounted to $37.733 million to 30 June 2014.

5.47 As previously discussed[166], AGSVA charges other government entities to recoup the cost of the employee and contractor clearances they sponsor. As part of the November 2009 revised policy proposal, annual revenue targets were set for the payment of fees based on the anticipated demand for clearances. Table 5.5 indicates that there has been a significant revenue shortfall for each financial year since AGSVA's establishment compared to the targets.

Table 5.5: AGSVA annual revenue compared to targets

Annual reporting period	Revenue target	Total revenue raised	Percentage of target
2011–12	$9 792 530	$7 164 947	73.2
2012–13	$10 146 939	$7 638 110	75.3
2013–14	$10 541 135	$6 374 426	60.5

Source: ANAO analysis of AGSVA annual reports to SCNS and November 2009 revised proposal.

5.48 Recent security clearance fee increases and the decision to charge Defence industry for security clearances will generate additional revenue over time. Defence's Chief Security Officer announced in August 2014 that revenue raised by charging Defence industry for security clearances 'will be used to build vetting capacity and enhance [AGSVA's] service delivery.'[167]

166 See paragraph 2.26.

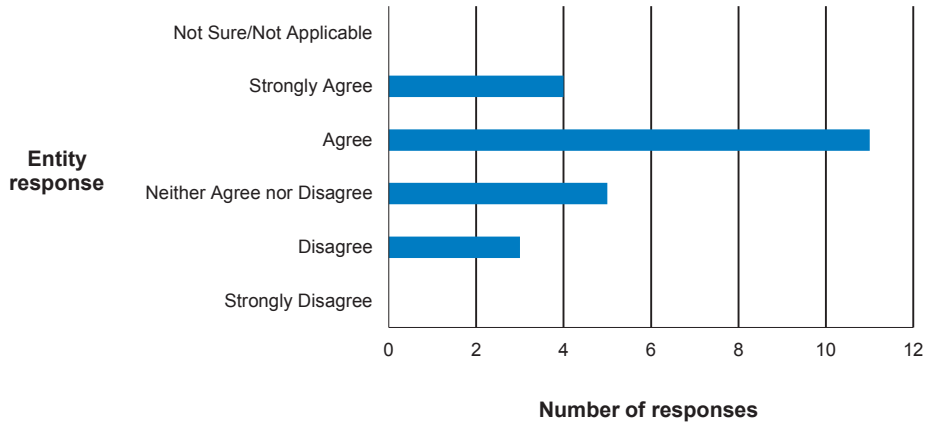
167 Defence, Defence Security Authority, Advice to Defence Industry: *Defence to Charge Industry for Security Vetting Services from 1 January*, 20 August 2014.

Entity Questionnaire results

5.49 Surveys can be a useful tool for customer service organisations in gauging the level of satisfaction with the services they provide, and identifying opportunities for improvement. As part of this audit, the ANAO sought feedback from selected government entities about the efficiency and effectiveness of AGSVA security vetting services. The ANAO's September 2014 Questionnaire was distributed to 30 Australian Government entities that receive security vetting services from AGSVA and are subject to the PSPF.[168] The ANAO received 23 responses.

5.50 Entity responses to the ANAO Questionnaire were mostly positive about some aspects of AGSVA's security vetting services. Sixty-five per cent of respondents agreed that AGSVA provides an efficient and effective vetting service for new security clearances (Figure 5.4), and 78 per cent of respondents agreed that AGSVA's vetting services had improved over the past two years. Fourteen of the 23 respondents[169] (61 per cent) provided additional comments that were positive about aspects of AGSVA's vetting services. These comments primarily focused on the improvement of services over the past two years.

Figure 5.4: Entity feedback on whether AGSVA provides an efficient and effective vetting service for new security clearances

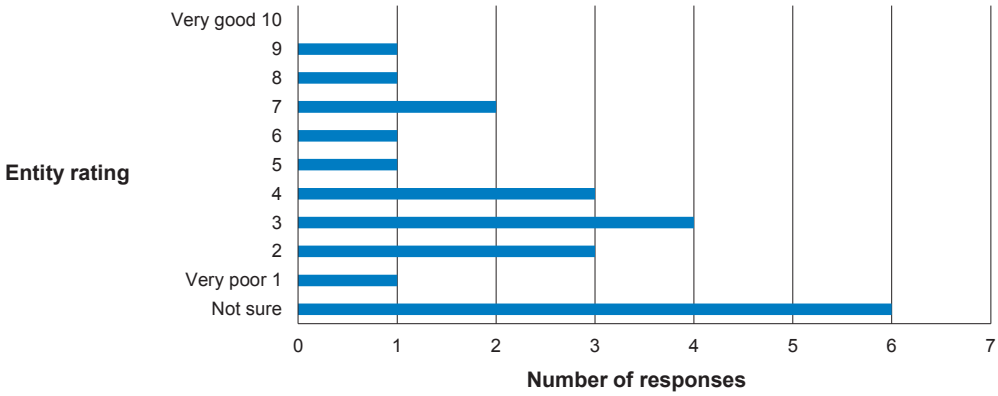


Source: September 2014 ANAO Questionnaire.

168 The entities included a mix of Departments of State and selected Portfolio Bodies.
169 Two entities did not provide any additional comments.

5.51 The ANAO Questionnaire contained a section on the timeliness of various AGSVA services. The majority of responses in this section were positive. However, responses to questions about the timeliness of AGSVA's management of revalidations, complex cases and changes of circumstance were mixed, with a number of entities rating AGSVA's performance in these areas as below average. For example, in response to the question of AGSVA's timeliness in responding to complex cases, 11 respondents (48 per cent) gave a rating of below five out of 10, and six respondents (26 per cent) were unsure (refer to Figure 5.5).

Figure 5.5: Entity feedback on AGSVA's ability to respond to complex cases in a timely manner



Source: September 2014 ANAO Questionnaire.

5.52 While there was positive commentary on AGSVA's recent service improvements, 20 of the 23 entities (87 per cent) provided comments that were critical of certain aspects of AGSVA's services and performance.[170] Several entities were concerned about AGSVA's communication, particularly when cases exceeded benchmark times or a clearance subject's case became more complex.

5.53 Several respondents indicated that AGSVA should provide more information when changes in a clearance subject's personal circumstances are actioned, or specific security vulnerabilities are identified during the vetting process. One response reflected concerns expressed by a number of entities:

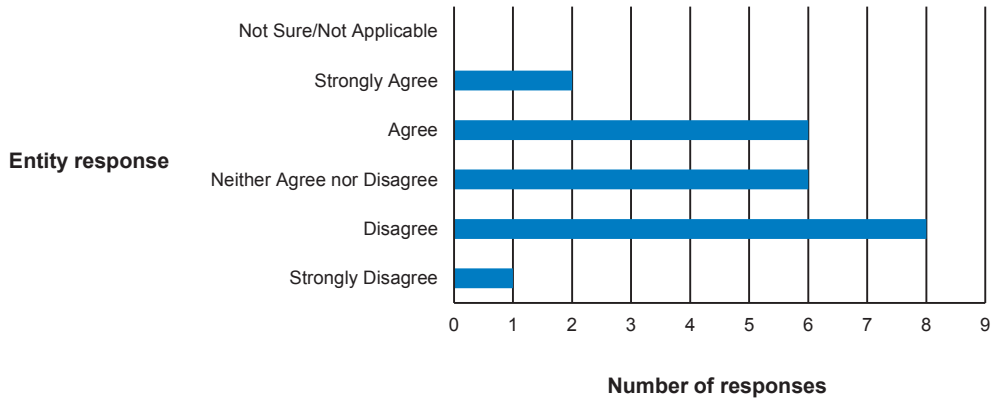
> To date AGSVA have not been able to inform us about complex cases or where the individual may not be suitable to hold a clearance for whatever reason.

170 Some responses included both positive and negative comments about AGSVA's service in a particular area. For example, several entities highlighted improvements in communication, but also suggested that communication was still a key issue for their entity.

> This was due to the uncertainty around privacy. AGSVA have subsequently advised our Department they can now inform us about complex matters and other information that may impact on an individual's ability to hold a clearance. This is yet to come through. This has made the mandatory requirements under the PSPF for "aftercare" arrangements very difficult since agency security staff had no visibility of possible security issues associated with staff.[171]

5.54 Effective ongoing management of clearances is dependent on effective communication and information sharing between the sponsoring entity and AGSVA.[172] Ongoing communication helps to ensure that all relevant information about a clearance holder's current situation is recorded and, where security concerns are identified that may impact on their suitability, such as past criminal behaviour, those concerns are properly managed. The ANAO Questionnaire resulted in mixed responses to the question of whether there was sufficient information sharing between AGSVA and the entity to effectively maintain security clearances. The results are displayed in Figure 5.6.

Figure 5.6: Entity feedback on whether there is sufficient information sharing between AGSVA and the entity to effectively maintain security clearances



Source: September 2014 ANAO Questionnaire.

171 Defence informed the ANAO that AGSVA seeks to strike the right balance between complying with the Australian Privacy Principles (and the broader Privacy Act), and meeting its obligation under the PSPF to share information about personnel security risk with relevant entities.

172 The Personnel Security Core Policy mandatory requirement, PERSEC 8, states that 'Agencies and vetting agencies must share information that may impact on an individual's ongoing suitability to hold an Australian Government security clearance.' AGD, *Australian Government Personnel Security Core Policy*, [Internet].

5.55 Nine of the 23 respondents to the ANAO Questionnaire suggested that improvements could be made to certain aspects of AGSVA vetting services. For example, several entities identified concerns with AGSVA's management of complex cases and change of circumstances processes, and suggested that improved communication would help to resolve their concerns. Several entities also suggested that an improved ePack user interface would help clearance subjects to complete their clearance packs in a timely manner.

5.56 AGSVA's Communications Strategy 2012–14 highlights the need to support two-way communication and enable voluntary feedback from government entities. In December 2014, during the course of this audit, AGSVA engaged an external contractor to conduct a survey of government entities and 4000 randomly selected clearance subjects to obtain feedback on its service delivery. AGSVA informed the ANAO that it intends to draw on the survey results to inform its 2015 External Communications Strategy, due to be finalised in April 2015. AGSVA also informed the ANAO that it now intends to conduct a survey of government entities and clearance subjects annually. Periodic surveys should help inform AGSVA's planning and strengthen the overall service delivery framework. The proposed surveys will also augment AGSVA's other feedback mechanisms, such as compliments and complaints received through its customer feedback register.

Conclusion

5.57 The AGSVA *Service Delivery Charter* includes four KPIs that address different aspects of vetting service delivery. One of these KPIs measures the timeliness of AGSVA's vetting process, with AGSVA aiming to complete 95 per cent of clearance cases within agreed benchmark timeframes. However, there is no apparent relationship between the 95 per cent target and the proportion of complex vetting cases which require additional information and review. The remaining KPIs do not measure the effectiveness of AGSVA's service delivery to inform management decision making. Reflecting the weaknesses in its KPIs, AGSVA's public reporting in the Defence Annual Report has been opaque and has not clearly conveyed the agency's performance in delivering whole-of-government vetting services over time.

5.58 Since its inception in October 2010, AGSVA has been unable to meet its 95 per cent target for processing security clearances within benchmark times, with around 45 per cent of clearances in 2013–14 processed in timeframes exceeding the relevant benchmark. Further, AGSVA has given priority to the

processing of initial clearances to enable employees and contractors to start work on behalf of entities, resulting in a backlog of some 13 000 clearance revalidations at current clearance levels. As mentioned in chapter 2, Defence has not developed a pathway 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.

5.59 Twenty-three Australian Government entities provided feedback on AGSVA's service delivery in response to the ANAO's September 2014 Questionnaire. While 78 per cent of the respondents agreed that AGSVA's vetting services had improved over the past two years, respondents also raised concerns about aspects of AGSVA's performance, including the agency's communication of the status of complex cases and related findings. Effective ongoing management of clearances is dependent on communication and information sharing between the sponsoring entity and AGSVA. There would be benefit in AGSVA considering how best to provide feedback to entities on specific security concerns identified during the vetting process, such as past criminal behaviour, to facilitate entities' supervision of affected staff.

Ian McPhee

Canberra ACT

9 June 2015

Appendices

Appendix 1 Entity Response

GGD
26 MAY 2015
3.30

SENSITIVE

Australian Government
Department of Defence

Mr Dennis Richardson
Secretary

Air Chief Marshal Mark Binskin, AC
Chief of the Defence Force

SEC/OUT/2015/107
CDF/OUT/2015/574

Dr Tom Ioannou 26/5
Group Executive Director
Australian Nation Audit Office
GPO Box 707
CANBERRA ACT 2600

Dear Dr Ioannou

PROPOSED AUDIT REPORT ON CENTRAL ADMINISTRATION OF SECRUITY VETTING

Thank you for the opportunity to provide comment on the Section 19, Proposed Report provided to Defence on 27 April 2015.

Defence's proposed amendments, editorials and comments are included at **Enclosure 1**. The response to Requests for Information is at **Enclosure 2**. The Defence response to the proposed report is included at **Enclosure 3**, for inclusion in the published report. **Enclosure 4** sets out our response to the recommendations included in the proposed report.

Should you have any queries, please contact Mr Geoffrey Brown, Chief Audit Executive.

Yours sincerely

Dennis Richardson
Secretary

26 May 2015

M. D. BINSKIN, AC
Air Chief Marshal
Chief of the Defence Force

26 May 2015

PO Box 7900 Canberra BC ACT 2610 Telephone 02 626 52851 - Facsimile 02 6265 2375
SENSITIVE
***Defending Australia** and its National Interests*

Appendix 2 Mandatory Requirements for Personnel Security

Requirement	Description
PERSEC 1	Agencies must ensure that their personnel who access Australian Government resources (people, information and assets): • are eligible to have access • have had their identity established • are suitable to have access • agree to comply with the government's policies, standards, protocols and guidelines that safeguard the agency's resources from harm.
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: • justify an exceptional business requirement • conduct and document a risk assessment • define the period covered by the waiver (which cannot be open-ended) • gain agreement from the clearance applicant to meet the conditions of the waiver, and • consult with the vetting agency.
PERSEC 6	Agencies, other than authorised vetting agencies, must use the Australian Government Security Vetting Agency (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: • inform vetting agencies when a clearance holder leaves agency employment or contract engagement • advise vetting agencies of any security concerns.

Source: AGD, *Protective Security Core Policy*, September 2014.

Appendix 3 Factors Considered When Assessing an Individual's Suitability to Hold a Clearance

1. The Attorney-General's Department *Personnel Security Guidelines, Vetting Practices* identifies factors to be considered when assessing an individual's suitability to hold a clearance, which are outlined below.

2. A clearance subject is suitable to hold a security clearance at any level, where it is established, to the appropriate degree of satisfaction, that the clearance subject possesses and demonstrates an appropriate level of integrity, i.e., a soundness of character and moral principle. In the security context, integrity is defined as a range of character traits that a clearance subject **should** possess and demonstrate in order for the Government to have confidence in that clearance subject's ability to protect security classified resources. These character traits are:

- **honesty** – truthful and frank, and do not have a history of unlawful behaviour
- **trustworthiness** – responsibility and reliability and maturity
- **maturity** – capable of honest self-appraisal and able to cope with stress; age is not necessarily a good indicator of maturity
- **tolerance** - an appreciation of the broader perspective even when holding strong personal views, able to remain impartial and flexible (an inability to accept other peoples' life choices or respect cultures can indicate intolerance); and accept differences in people, opinions or situations through respect, understanding and empathy
- **resilience** – ability to adapt well in the face of adversity, trauma, tragedy, threats or significant sources of stress, and
- **loyalty** – a commitment to the democratic processes of the Australian Government, loyalty is not confined to the nation but also includes the objectives, ethos and values of the working environment (strong political views incompatible with the Australian Constitution may put in doubt a person's loyalty).

3. Reference to a number of factor areas of the clearance subject's life, including personal relationships, employment history, behaviour and financial habits contributes to an assessment of a clearance subject's integrity. Agencies

should be confident that clearance subjects who are responsible for security classified resources possess a sound and stable character.

4. Clearance subjects must also demonstrate that they are not unduly vulnerable to influence or coercion.[173]

173 AGD, *Personnel security guidelines, Vetting Practices,* Version 1.0, 4 November 2014, pp. 34–35.

Index

Series Titles

ANAO Report No.1 2014–15
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2013 Compliance)
Across Agencies

ANAO Report No.2 2014–15
Food Security in Remote Indigenous Communities
Department of the Prime Minister and Cabinet

ANAO Report No.3 2014–15
Fraud Control Arrangements
Across Entities

ANAO Report No.4 2014–15
Second Follow-up Audit into the Australian Electoral Commission's Preparation for and Conduct of Federal Elections
Australian Electoral Commission

ANAO Report No.5 2014–15
Annual Compliance Arrangements with Large Corporate Taxpayers
Australian Taxation Office

ANAO Report No.6 2014–15
Business Continuity Management
Across Entities

ANAO Report No.7 2014–15
Administration of Contact Centres
Australian Taxation Office

ANAO Report No.8 2014–15
Implementation of Audit Recommendations
Department of Health

ANAO Report No.9 2014–15
The Design and Conduct of the Third and Fourth Funding Rounds of the Regional Development Australia Fund
Department of Infrastructure and Regional Development

ANAO Report No.10 2014–15
Administration of the Biodiversity Fund Program
Department of the Environment

ANAO Report No.11 2014–15
The Award of Grants under the Clean Technology Program
Department of Industry

ANAO Report No.12 2014–15
Diagnostic Imaging Reforms
Department of Health

ANAO Report No.13 2014–15
Management of the Cape Class Patrol Boat Program
Australian Customs and Border Protection Service

ANAO Report No.14 2014–15
2013–14 Major Projects Report
Defence Materiel Organisation

ANAO Report No.15 2014–15
Administration of the Export Market Development Grants Scheme
Australian Trade Commission

ANAO Report No.16 2014–15
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2014
Across Entities

ANAO Report No.17 2014–15
Recruitment and Retention of Specialist Skills for Navy
Department of Defence

ANAO Report No.18 2014–15
The Ethanol Production Grants Program
Department of Industry and Science

ANAO Report No.19 2014–15
Management of the Disposal of Specialist Military Equipment
Department of Defence

ANAO Report No.20 2014–15
Administration of the Tariff Concession System
Australian Customs and Border Protection Service

ANAO Report No.21 2014–15
Delivery of Australia's Consular Services
Department of Foreign Affairs and Trade

ANAO Report No.22 2014–15
Administration of the Indigenous Legal Assistance Programme
Attorney-General's Department

ANAO Report No.23 2014–15
Administration of the Early Years Quality Fund
Department of Education and Training
Department of Finance
Department of the Prime Minister and Cabinet

ANAO Report No.24 2014–15
Managing Assets and Contracts at Parliament House
Department of Parliamentary Services

ANAO Report No.25 2014–15
Administration of the Fifth Community Pharmacy Agreement
Department of Health
Department of Human Services
Department of Veterans' Affairs

ANAO Report No.26 2014–15
Administration of the Medical Specialist Training Program
Department of Health

ANAO Report No.27 2014–15
Electronic Health Records for Defence Personnel
Department of Defence

ANAO Report No.28 2014–15
Management of Interpreting Services
Department of Immigration and Border Protection
Department of Social Services

ANAO Report No.29 2014–15
Funding and Management of the Nimmie-Caira System Enhanced Environmental Water Delivery Project
Department of the Environment

ANAO Report No.30 2014–15
Materiel Sustainment Agreements
Department of Defence
Defence Materiel Organisation

ANAO Report No.31 2014–15
Administration of the Australian Apprenticeships Incentives Program
Department of Education and Training

ANAO Report No.32 2014–15
Administration of the Fair Entitlements Guarantee
Department of Employment

ANAO Report No.33 2014–15
Organ and Tissue Donation: Community Awareness, Professional Education and Family Support
Australian Organ and Tissue Donation and Transplantation Authority

ANAO Report No.34 2014–15
Administration of the Natural Disaster Relief and Recovery Arrangements by Emergency Management Australia
Attorney-General's Department

ANAO Report No.35 2014–15
Delivery of the Petrol Sniffing Strategy in Remote Indigenous Communities
Department of the Prime Minister and Cabinet

ANAO Report No.36 2014–15
Administration of the Assistance for Isolated Children Scheme
Department of Human Services

ANAO Report No.37 2014–15
Management of Smart Centres' Centrelink Telephone Services
Department of Human Services

ANAO Report No.38 2014–15
Administration of Enforceable Undertakings
Australian Securities and Investments Commission

ANAO Report No.39 2014–15
Promoting Compliance with Superannuation Guarantee Obligations
Australian Taxation Office

ANAO Report No.40 2014–15
Transport Services for Veterans
Department of Veterans' Affairs

ANAO Report No.41 2014–15
The Award of Funding under the Safer Streets Programme
Attorney-General's Department

ANAO Report No.42 2014–15
Administration of Travel Entitlements Provided to Parliamentarians
Department of Finance

ANAO Report No.43 2014–15
Managing Australian Aid to Vanuatu
Department of Foreign Affairs and Trade

ANAO Report No.44 2014–15
Interim Phase of the Audits of the Financial Statements of Major General Government Sector Entities for the year ending 30 June 2015
Across Entities

ANAO Report No.45 2014–15
Central Administration of Security Vetting
Department of Defence

Better Practice Guides

The following Better Practice Guides are available on the ANAO website:

Public Sector Financial Statements: High-quality reporting through good governance and processes	Mar. 2015
Public Sector Audit Committees: Independent assurance and advice for Accountable Authorities	Mar. 2015
Successful Implementation of Policy Initiatives	Oct. 2014
Public Sector Governance: Strengthening performance through good governance	June 2014
Administering Regulation: Achieving the right balance	June 2014
Implementing Better Practice Grants Administration	Dec. 2013
Human Resource Management Information Systems: Risks and Controls	June 2013
Public Sector Internal Audit: An Investment in Assurance and Business Improvement	Sept. 2012
Public Sector Environmental Management: Reducing the Environmental Impacts of Public Sector Operations	Apr. 2012
Developing and Managing Contracts: Getting the Right Outcome, Achieving Value for Money	Feb. 2012
Fraud Control in Australian Government Entities	Mar. 2011
Strategic and Operational Management of Assets by Public Sector Entities: Delivering Agreed Outcomes through an Efficient and Optimal Asset Base	Sept. 2010
Planning and Approving Projects – an Executive Perspective: Setting the Foundation for Results	June 2010
Innovation in the Public Sector: Enabling Better Performance, Driving New Directions	Dec. 2009
SAP ECC 6.0: Security and Control	June 2009
Business Continuity Management: Building Resilience in Public Sector Entities	June 2009
Developing and Managing Internal Budgets	June 2008