The Auditor-General
Audit Report No.41 2007–08
Performance Audit

# Management of Personnel Security—Follow-up Audit

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 81023 0

**COPYRIGHT INFORMATION**

Australian National
Audit Office

Canberra ACT
18 June 2008

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit across agencies in accordance with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit and the accompanying brochure to the Parliament. The report is titled *Management of Personnel Security—Follow-up Audit.*

Following its tabling in Parliament, the report will be placed on the Australian National Audit Office's Homepage—http://www.anao.gov.au.

Yours sincerely

Steve Chapman

Steve Chapman
Acting Auditor-General

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

**AUDITING FOR AUSTRALIA**

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

**Telephone: (02) 6203 7505**
**Fax: (02) 6203 7519**
**Email: webmaster@anao.gov.au**

ANAO audit reports and information about the ANAO are available at our internet address:

http://www.anao.gov.au

## Audit Team

Russell Eade
Bill Bonney
Rowena Carne
Andrew Morris

# Contents

# Abbreviations

| | |
|---|---|
| AGD | Attorney-General's Department |
| ANAO | Australian National Audit Office |
| APRA | Australian Prudential Regulation Authority |
| ASA | Agency Security Adviser |
| BSP | Business Support Process |
| CSIRO | Commonwealth Scientific and Industrial Research Organisation |
| Defence | Department of Defence |
| DIAC | Department of Immigration and Citizenship |
| DSAP | Designated Security Assessment Position |
| Finance | Department of Finance and Deregulation |
| HRMIS | Human Resource Management Information System |
| ICT | Information and Communications Technology |
| JCPAA | Joint Committee of Public Accounts and Audit |
| PoT | Position of Trust |
| PSCC | Protective Security Coordination Centre |
| PSM | Australian Government Protective Security Manual (2005) |

# Glossary

Personnel security

Policies and practices used in managing risks inherent in allowing people to access security classified information or resources.

Portability

The principle that security clearances conducted in accordance with the minimum requirements of the PSM should be recognised by all Australian Government organisations.

Position assessment

Assessment of duties and tasks to be performed in each position, role or function to determine if the occupant of the position requires access to classified material and therefore a security clearance.

Protective security

A broad concept covering information, personnel, and physical security.

Security aftercare

Processes for early identification of issues related to an individual's continued suitability to hold a security clearance.

Security awareness

Understanding and appreciating potential risks and threats to, and the costs of, the loss or compromise of information or assets, and accepting the responsibilities and obligations to address those issues.

Security classified information

Official information that must be afforded a level of protection to safeguard it from compromise or unauthorised use because it could cause harm, or have adverse consequences.

Security clearance process

The process of assessing individuals' eligibility and suitability for access to security classified information through a comprehensive evaluation of their history, attitudes, values and behaviour.

Security risk

An event that could result in the compromise of official resources. Security risks are measured in terms of their probability and consequences.

Suitability indicators

Factors considered in security clearances assessments such as maturity, responsibility, tolerance, honesty and loyalty.

# Summary and Recommendations

# Summary

## Introduction

1. Personnel security describes the policies and practices used in managing the risks inherent in allowing Australian government employees and other personnel access to security classified information or resources. The central tenet of personnel security is that access to sensitive information is restricted to people with a legitimate requirement and who are reliable and aware of their responsibilities to protect such information.

2. Personnel security is an integral part of the framework used by Australian Government organisations to protect official information and resources. As such, effective personnel security requires a comprehensive and coordinated approach that complements other elements of protective security, particularly: physical security; information security, including information and communications technology (ICT) holdings; security in procurement and contracting; and the management of security incidents and investigations.

3. The Australian Government Protective Security Manual (PSM) sets out protective security policy and minimum procedural requirements for Australian Government organisations.[1] Part D of the PSM contains policies and standards relating to personnel security, including standards for the conduct and maintenance of security clearances.

4. Responsibility for the development, implementation and maintenance of effective personnel security functions lies with the chief executive of each organisation. In many organisations, this responsibility is exercised by a personnel security executive, supported by a security adviser and a team of dedicated security clearance staff.

[1] Attorney-General's Department, *Australian Government Protective Security Manual*, Canberra, August 2005. The PSM applies to all agencies subject to the *Financial Management and Accountability Act 1997* (FMA Act), and applies to bodies that are subject to the *Commonwealth Authorities and Companies Act 1997* (CAC Act) which have received notice in accordance with that Act that the Manual applies to them as a general policy of the Australian Government.

## Determining security clearance requirements

5. According to the PSM, there are two categories of security classified information or resources—national security and non-national security.[2] The PSM describes people requiring access to national security classified information as having a Designated Security Assessment Position (DSAP), and those requiring access to non-national security classified information as being in a Position of Trust (PoT). In this context, a person's eligibility to access security classified information is dependent on:

- a demonstrable 'need to know'—the person will, or may be required to, access security classified information or resources in the course of carrying out their official duties; and
- the conduct of a security clearance—a comprehensive review to confirm the person's identity and assess their suitability to access security classified information.

6. The level of security clearance required should be determined by reference to the duties and tasks to be performed, including the security classification of the information that may be accessed. Judgements made concerning a person's eligibility for a security clearance should be subject to ongoing monitoring.

## Previous audit coverage

7. Since 2002, three reports have been produced by the Australian National Audit Office (ANAO) and the Joint Committee of Public Accounts and Audit (JCPAA) that assessed the adequacy of personnel clearance arrangements in Australian Government organisations. These three reports were:

- ANAO Audit Report No.22 2001–02, *Personnel Security—Management of Security Clearances*, which made 10 recommendations to assist organisations improve personnel security arrangements;
- JCPAA Report 390, *Review of Auditor General's Reports 2001–02*, which supported the ANAO's findings in Audit Report No.22 2001–02 and made three additional recommendations concerning personnel security; and

[2] National security describes official information which, if compromised, could affect the security of Australia, including its defence systems or operations, international relations or national interests. Non-national security describes official information which, if compromised, does not threaten the security of Australia, but which could threaten the security or interests of individuals, groups, commercial entities, or the safety of the community.

- ANAO Audit Report No.15 2003–04, *Administration of Staff Employed under the Members of Parliament (Staff) Act 1984* (MOP(S) Act), of which Recommendation No. 1 proposed that the (then) Department of Finance and Administration (Finance) improve processes to encourage MOP(S) Act staff to gain security clearances.

8. As indicated above, these three reports[3] made a total of 14 recommendations for improving personnel security arrangements at Australian Government organisations. All recommendations in the two audit reports were agreed by all participating organisations.[4]

## Audit approach

### Audit objective, scope and criteria

9. The objective of this audit was to assess the effectiveness of personnel security arrangements at selected Australian Government organisations, including whether they satisfied the requirements of the PSM.

10. To address this objective, the audit examined the extent to which the selected organisations implemented the 14 recommendations from the three previous reports (outlined in paragraph 7).

11. These recommendations represent the audit criteria. The audit scope also takes into account the update of the PSM from the 2000 version applying at the time of the previous audit to the current version released in August 2005.

### Audit coverage and methodology

12. Personnel security arrangements at four Australian Government organisations were assessed against all ten recommendations from ANAO Audit Report No.22 2001–02 and two of the additional recommendations from JCPAA Report 390.[5] These four organisations were:

- Australian Prudential Regulation Authority (APRA);

[3] These three reports are referred to, in some instances, as the previous reports.

[4] Australian Government organisations are not required to provide a formal response as to whether they agree or disagree with recommendations proposed by the JCPAA.

[5] The two relevant recommendations were Recommendation No. 7, regarding the level of resources allocated to the conduct and administration of security clearances, and Recommendation No. 8 regarding the management of personnel security information.

- Commonwealth Scientific and Industrial Research Organisation (CSIRO);
- Department of Defence (Defence); and
- Department of Immigration and Citizenship (DIAC).

13. These four organisations processed around 39 000 clearances between January 2005 and November 2007 and, in total, had approximately 125 000[6] active security clearances.[7] The ANAO held interviews with key staff at these organisations, and reviewed relevant documentation including policy and related guidance material, security risk assessments, security awareness and training programs, and management reports outlining personnel security performance. The ANAO also examined a sample of security clearances granted between January 2005 and November 2007 at these organisations.

14. The audit also assessed the extent to which:

- the Attorney-General's Department (AGD) had implemented Recommendation No. 9 in JCPAA Report 390, which proposed that AGD report on the cost-effectiveness of maintaining a central database of security clearances; and
- as reported in paragraph 7, Finance had implemented Recommendation No. 1 from ANAO Audit Report No.15, 2003–04, regarding security clearances for MOP(S) Act staff.

15. Following the conduct of audit fieldwork, all six selected organisations were provided with a management report detailing audit findings, conclusions and, in some instances, recommendations for improvement.

## Audit conclusion

16. Part D of the PSM (2005) provides an effective framework for the administration of personnel security. In particular, it provides extensive guidance and sets minimum standards across the key elements of managing personnel security functions, and conducting and maintaining security clearances. Most of the recommendations from the previous reports related to

[6] One organisation had approximately 90 per cent of this total.

[7] These organisations granted security clearances to over 99 per cent of all individuals requiring clearances between January 2005 and November 2007. Rather than deny a clearance, organisations can adequately protect information through more moderate approaches, such as granting the security clearance subject to conditions, downgrading the clearance to a lower level or changing the duties of the individual to avoid the need for a security clearance.

the application of the minimum standards of the PSM regarding personnel security.

17. Two of the selected organisations had fully implemented almost all recommendations from the previous reports. These findings demonstrate that organisations with a strong focus on personnel security, including the allocation of sufficient resources, are more likely to have effective personnel security arrangements and satisfy the relevant minimum requirements of the PSM. Typically this focus involves:

- demonstrated commitment by, and regular reporting of personnel security performance to, senior management;
- a sound understanding throughout the organisation of personnel security risks and threats;
- actively managing security clearance review requirements; and
- delivery of formal and structured security awareness training, including training on personnel security responsibilities.

18. Conversely, two organisations had not fully implemented most of the recommendations from the previous reports. These findings indicate that those organisations without a mature personnel security function, or that had not paid sufficient attention to the specific requirements of the PSM, are unlikely to have effective personnel security arrangements. In particular, the audit identified weaknesses in:

- the management of personnel security risks, including processes to regularly assess security clearance requirements; and
- the timely identification and assessment of issues impacting on an individual's continued suitability to hold a security clearance (security aftercare).

19. The ANAO concludes that while there has been a general improvement in the administration of personnel security since the previous reports, there remains considerable scope for some organisations to improve many key personnel security processes.

20. In terms of the three main themes in personnel security—managing the personnel security function, and conducting and maintaining security clearances, overall the selected organisations had:

- partially implemented the requirements of the PSM in managing the personnel security function. The organisations generally did not have effective risk-management approaches in relation to personnel security. They also had not reviewed and revised relevant policy and procedural guidance against all key relevant aspects of the revised PSM;
- substantially implemented the requirements of the PSM when undertaking processes associated with conducting security clearances; [8] and
- substantially implemented the requirements of the PSM in maintaining security clearances,[9] except for providing adequate security aftercare.

21. A particular concern raised by the JCPAA and ANAO in previous reports was the extent of backlogs of security clearance re-evaluations.[10] The current audit found a substantial improvement in this regard, and at the time of the audit, the selected organisations had minimal or no backlogs of security clearance reviews.

22. Similarly, improved administrative processes at Finance helped to reduce the backlog of security clearances for MOP(S) Act staff over the period May 2005 to November 2007 from a high of 45 per cent in May 2006 to a low of 16 per cent in November 2007, although this level remained higher than in the Australian Government organisations examined.[11]

## Key findings

23. Key findings from the audit are outlined below according to the three main themes in personnel security—managing the personnel security function, and conducting and maintaining security clearances.

[8] These processes included managing contractors, documenting security clearances assessments and utilising organisation-specific risk factors as part of these assessments.

[9] These processes included managing security review requirements and providing awareness programs and training.

[10] JCPAA Report 390, *Review of Auditor-General's Reports 2001–02*, p. 58. Further, ANAO Report No.22 2001–02, *Personnel Security—Management of Security Clearances*, p. 51, reported that the proportion of out-of-date security clearances in the selected organisations ranged from 'zero to around 10 per cent of total security clearances (in the best cases) and up to around 40 per cent (in the worst cases)'.

[11] As a result of the Federal election held on 24 November 2007, security clearances for MOP(S) Act staff employed by the previous government were suspended by Finance. Finance has commenced processing security clearances for the staff of the new government. This is likely to create a short-term increase in workload and also impact on the timeliness of clearance processing by the contracted security clearance providers.

## Managing the personnel security function (Chapter 2)

24. Key factors underpinning the effective management of personnel security functions include: comprehensive policy and guidance material; an understanding of potential risks; identifying and monitoring security clearance requirements; and access to accurate information to support decision-making. In this context, the audit examined the extent to which the selected organisations implemented: Audit Report No.22 2001–02, Recommendations No. 1, 2, 3 and 7; Audit Report No.15 2003–04, Recommendation No. 1; and JCPAA Report No. 390, Recommendation No. 8.

### *Policy and procedures*

Audit Report No.22 2001–02, Recommendation No. 1

The ANAO recommends organisations approve and promulgate appropriate policy and procedures to support the conduct and administration of personnel security. In this regard, policy and procedures should be based on, but not necessarily limited to, the policy and guidance material contained in PSM (2000).

Finding of the current audit

*One* of the selected organisations had *fully* implemented this recommendation, *two* had *substantially* implemented it, and the *other* had *partially* implemented it.

25. Each of the selected organisations had promulgated a series of policy and procedural documents relating to their personnel security functions. This material varied in detail and usefulness between organisations, but for the most part was informative and helpful to staff.

26. Since the previous audit, the PSM has been revised, and the current version contains considerably more prescription and guidance on personnel security than the previous version published in 2000.[12] Despite these considerable changes, none of the selected organisation had systematically assessed the appropriateness of each of their policies, procedures and guidance documentation in light of the release of the revised PSM in 2005. At the time of the audit, three organisations had initiated but not completed such reviews.

[12] For example, the number of mandatory minimum standards in Part D increased from 36 in the 2000 version to approximately 120 in the 2005 version.

### *Security risk management*

Audit Report No.22, 2001–02, Recommendation No. 2

The ANAO recommends organisations review their security risk management processes against the requirements of Part B of PSM (2000) and, in particular, ensure:

- personnel security threats and hazards are thoroughly considered in this process; and
- organisation-specific security risks are factored into the security clearance process, as appropriate.

*One* organisation had *fully* implemented this recommendation, *two* had *partially* implemented it, and the *other* had *not* implemented it.

27. Three organisations had policies and processes in place to identify, assess and manage security risks. However, the ANAO considered that only one organisation had an adequate record of risks, and attendent risk-mitigation controls, associated with its personnel security function.[13]

28. One organisation had not systematically reviewed risks and associated controls it had identified in a security risk assessment undertaken early in 2005. In the absence of such an assessment, there was considerable uncertainty as to whether the organisation was properly informed about new or emerging risks. Another organisation did not have a current risk assessment for its personnel security operations.

29. At the time of the audit, the remaining organisation had not assessed, and did not have a framework for managing, security risks.

### *Position assessments*[14]

Audit Report No.22 2001–02, Recommendation No. 3

The ANAO recommends:

- registers of Designated Security Assessment Positions (DSAP) and Positions of Trust (PoT) are reviewed periodically to ensure they accurately reflect the organisation's continued security clearance requirements; and
- organisations develop appropriate guidelines to assist managers to undertake position assessments.

[13] In 2007, that organisation undertook a systematic review of potential threats across each dimension of protective security, such as assessing the potential impact of a range of risks to its personnel security functions, including the conduct of security clearances.

[14] Assessment of duties and tasks to be performed in each position, role or function to determine if the occupant of the position requires access to classified material and therefore a security clearance.

*One* organisation had *fully* implemented this recommendation, *two* had *substantially* implemented it, and *one* had *partially* implemented it.

30. Two organisations had formal processes for identifying, recording and maintaining security clearance requirements for each position in their establishment. At both organisations, information obtained from these processes provided the basis for the conduct of security clearances. However, only one organisation utilised its Human Resource Management Information System (HRMIS) to record, approve and monitor the currency of security clearance requirements for each position.

31. Most security clearance requirements at one organisation were driven by decisions to require certain staff to have SECRET level clearances. In the remaining organisation, the need for security clearances was largely determined on a case-by-case basis depending on the clearance subject's duties.

### *Information management*

Audit Report No.22 2001–02, Recommendation No. 7

To improve the effectiveness of security information management, the ANAO recommends organisations assess opportunities to integrate the management of personnel (including contractor) security information into the organisation's HRMIS or other appropriate corporate system.

JCPAA Report 390, Recommendation No. 8

The JCPAA recommends all agencies make the necessary changes to their HRMIS to support management reporting in relation to security clearances and appropriate access to security clearance information.

*Two* organisations had *fully* implemented ANAO Recommendation No. 7, *one* had *substantially* implemented it and *one* had *partially* implemented it.

*Two* organisations had *fully* implemented JCPAA Recommendation No. 8, *one* had *not* implemented it, and it *did not apply* to the *other*.

32. Two organisations either integrated personnel security information with, or had adequate links to relevant information in, a HRMIS, while two organisations did not use a HRMIS. Of the two that had not, one organisation had commenced a program to provide adequate integration, and the other had so few clearances that integration was not warranted.

33. The organisations which had integrated personnel security information into their HRMIS, and the organisation with links between personnel security information and the HRMIS, were the only ones that actively monitored

information on the performance of the personnel security function, including the security clearance workload. In both cases, details of performance were regularly provided to the organisation's senior executives.

### *Monitoring security clearances for MOP(S) Act staff*

**Audit Report No.15 2003–04, Recommendation No. 1**

The ANAO recommends Finance strengthen monitoring procedures to ensure MOP(S) Act staff with outstanding security clearances are identified in a timely manner, and that appropriate follow--up is undertaken with relevant staff members, their employing Parliamentarians and the security vetting agency undertaking the security clearances.

*Finance* has implemented this recommendation.

**34.** Finance had enhanced its administration of security clearances for MOP(S) Act staff, including by: improving the measurement and reporting of performance; and adopting more structured processes for following-up outstanding clearance packs, including introducing a formal non-compliance process for those staff who do not submit the necessary forms within a pre-determined time period.[15]

**35.** The proportion of clearances reported as outstanding in November 2007 (16 per cent) was the smallest since the previous audit. The ANAO considers that this result reflects improvements made by Finance in the administration of these security clearances.

## Conducting security clearances (Chapter 3)

**36.** In conducting a security clearance, an organisation must obtain and evaluate sufficient information to be reasonably assured of an individual's responsibility, integrity and maturity, in light of an individuals' prospective position and the organisation's risk and threat environment. Specifically, the ANAO examined the extent to which the selected organisations implemented Audit Report No.22 2001–02, Recommendations No. 4, 5 and 6; and JCPAA Report 390, Recommendation No. 9.

[15] This non-compliance process establishes a timeframe of 12 weeks for MOP(S) Act staff to submit their completed security clearance packs. If packs are not provided within that period, Finance commences a clearance denial process.

### *Contract management*

Audit Report No.22 2001–02, Recommendation No. 4

The ANAO recommends organisations adopt better practice contract management principles and standards in outsourced security clearance and vetting service arrangements.

*All three* organisations with outsourced arrangements had *substantially* implemented this recommendation.

37. The three organisations with outsourced arrangements had effectively managed the workload and timeliness of external providers conducting security clearances. The major shortcoming in the contracts was that they lacked information on measuring the performance of contractors, including identifying specific performance indicators.

38. ANAO testing found however that external providers typically conducted security clearance assessments to a high standard, as reflected in comprehensive documentation contained on personal security files.

### *Documenting security clearance assessments*

Audit Report No.22 2001–02, Recommendation No. 5

The ANAO recommends organisations record all information collected during the course of a security clearance on an individual's personal security file.

*Three* organisations had *fully* implemented this recommendation and the *other* had *partially* implemented it.

39. The examination of security clearances found that all but one of the four organisations had recorded sufficient information on individuals' personal security files to fully justify the decision to grant security clearances.

40. The main shortcomings identified in the other organisation were that: none of the personal security files contained a formal request for security clearance; approximately 12 per cent of personal security files did not contain a copy of the clearance subject's full birth certificate; around 24 per cent of the copies of birth certificates and 15 per cent of the copies of marriage certificates were not properly certified; and there was a general lack of evidence to indicate that the clearance subject's background had been assessed.

### *Suitability indicators*

**Audit Report No.22 2001–02, Recommendation No. 6**

The ANAO recommends organisations develop suitability indicators for use in security clearance assessments that are informed by organisation-specific risk factors.

*Two* organisations had *fully* implemented this recommendation, *one* had *partially* implemented it and the *other* had *not* implemented it.

**41.** ANAO testing of security clearances found an appropriate level of evidence of the consideration or assessment of suitability in two of the selected organisations. One of these organisations advised that it had recently introduced a new form for use in the conduct of security clearances which required officers to explicitly make an assessment against a range of suitability factors and, as necessary, develop a risk management regime to deal with any concerns.

**42.** The ANAO found there was generally insufficient evidence available to indicate that the suitability of clearance subjects had been evaluated during security clearance process in one organisation.

### *Portability of security clearances*

**JCPAA Report 390, Recommendation No. 9**

The Committee recommends the Attorney-General's Department report to the Committee on the cost-effectiveness of maintaining a central database of security clearances**.**

The Attorney-General's Department implemented this recommendation.

**43.** In November 2003, AGD formally responded to the above recommendation, concluding: 'there are fundamental reasons why such an approach … would not be effective'. AGD advised the JCPAA that the issue of portability would be addressed as part of a comprehensive review of existing personnel security policy. This review culminated in the release of the upgraded PSM in August 2005.

**44.** The ANAO considers that enhancements to the PSM released in 2005 provide a sound framework for improving the portability[16] of security clearances amongst Australian Government organisations.

[16] Portability refers to the transfer of an individual's security clearance between Australian Government organisations.

45. The ANAO notes that concerns remain about the portability of security clearances, particularly clearances for contracted service providers. In this regard, AGD is currently examining the feasibility of a central record of clearances for ICT professionals. The results of this work should enable AGD to identify and assess opportunities of using a centralised system to record and administer Australian Government security clearances more broadly.

## Maintaining security clearances (Chapter 4)

46. Effective maintenance of security clearances involves: promoting security awareness throughout the organisation; periodically reviewing each security clearance; and monitoring any issues impacting on the continued suitability of a clearance subject to hold a security clearance. In this context, the ANAO examined the extent to which the selected organisations implemented Audit Report No.22 2001–02, Recommendations No. 8, 9 and 10; and JCPAA Report 390, Recommendation No. 7.

### *Security clearance reviews*

Audit Report No.22 2001–02, Recommendation No. 8

It is recommended organisations consider taking concerted efforts to overcome the current backlog in the conduct of security clearance reviews as a matter of priority and ensure these processes are carried out in a timely manner in the future.

*Two* organisations had *fully* implemented this recommendation, *one* had *substantially* implemented it, and *one* organisation had *partially* implemented it.

47. The audit found a substantial improvement in the level of out-of-date security clearance reviews. In particular, two relatively large organisations that were included in the previous audit had considerably reduced the level of out-of-date security clearance reviews.

48. Two organisations did not have any overdue security clearance reviews at the time of the audit. At the other two organisations, the proportion of SECRET and TOP SECRET security clearance re-evaluations that were overdue at the time of the audit was relatively small—around five per cent in both cases. However, a number of these had been overdue for more than 12 months.

49. The audit found a significant improvement in processes used to manage security clearance reviews. For example, all of the selected organisations had arrangements in place to identify and action security clearance review requirements in a timely manner.

### *Resources*

JCPAA Report 390, Recommendation No. 7

The JCPAA recommends organisations allocate the resources necessary to bring their security clearance processes in line with the requirements of the PSM.

*Three* organisations had *fully* implemented this recommendation and *one* had *partially* implemented it.

50. Since the previous audit, three organisations had increased the level of resources allocated to the conduct and administration of security clearances. The remaining organisation outsourced its security clearance requirements and at the time of the audit, did not require any additional resources to meet its security clearance workload.

### *Security awareness*

Audit Report No.22 2001–02, Recommendation No. 9

The ANAO recommends organisations review the effectiveness of personnel security awareness and education programs to improve the identification, monitoring and promotion of personnel security issues.

*Three* organisations had *fully* implemented this recommendation and *one* had *partially* implemented it.

51. Three organisations had provided regular, structured personnel security awareness training to their staff, either face-to-face or through an on-line application. A range of measures were used at two organisations to complement formal training, including:

- regularly publishing a dedicated security newsletter;
- providing staff with a series of pamphlets and booklets setting out their various security responsibilities; and
- requiring certain staff to complete an on-line security awareness questionnaire.

52. The other organisation did not provide personnel security education or awareness training on a structured or regular basis. Rather, it was delivered irregularly as resources allowed. Furthermore, no records were kept of attendance at this training.

### *Security aftercare*

Audit Report No.22 2001–02, Recommendation No. 10

The ANAO recommends organisations review and improve the effectiveness of processes for the early identification of issues related to an individual's continued suitability to hold a security clearance.

*Two* organisations had *fully* implemented this recommendation while the other *two* had *not* implemented it.

53. Two organisations had a range of processes to manage the timely identification, and assessment, of issues related to an individual's continued suitability to hold a security clearance (security aftercare). These processes included: implementing tailored security aftercare management programs; providing clear instructions; and regularly reinforcing the requirement for staff to report changes in circumstances and contracts. In addition, both organisations regularly conducted security inspections.

54. Conversely, the two other organisations did not have clear security aftercare arrangements. In particular, they lacked formal processes, outside of clearance reviews, to systematically identify issues relevant to the ongoing suitability of individuals.

## Sound and better practices

55. Table 1 highlights examples of sound and better practices observed amongst the selected organisations.

### Table 1

### Sound and better practices

| **Managing personnel security** |
|---|
| Two organisations actively monitored the performance of the personnel security function, and regularly reported on this performance to senior executives. |
| One mid-size organisation had integrated personnel security information, including information on security clearance requirements (position assessments) into a HRMIS. |
| One organisation undertook a systematic review of potential threats across each dimension of protective security, including personnel security. That organisation had also formulated a security plan, which amongst other things, contained: a schedule of risk treatments; the identity of the official responsible for implementing each treatment; and details of monitoring arrangements. |
| **Conducting security clearances** |
| One organisation recently introduced a form for use in the conduct of security clearances which required officers to explicitly make an assessment against a range of suitability factors and, as necessary, develop a risk management regime to deal with any concerns. |
| **Maintaining security clearances** |
| One organisation monitored security clearance review requirements six months in advance of their due date. |
| One organisation had improved administration and associated workflow by allocating responsibility for the identification and management of security clearance reviews to a dedicated team. |
| One organisation required attendance at security awareness training to be included as a standard capability in all staff's performance agreements. |

Source: ANAO.

## Summary of organisations' responses to the audit

56. Each of the audited organisations agreed with the two recommendations.

# Recommendations

*The following recommendations are based on findings from fieldwork at the selected organisations and are likely to be relevant to other Australian Government organisations. Therefore, all Australian Government organisations should assess the benefits of implementing the recommendations in light of their own circumstances, including the extent that each recommendation, or part thereof, is addressed by practices already in place.*

| | |
|---|---|
| **Recommendation No. 1**<br>**Para 2.19** | The ANAO recommends that organisations regularly review personnel security risk assessments to identify new or emerging risks or changes in risk ratings, and assess the effectiveness of risk treatments. |
| **Recommendation No. 2**<br>**Para 4.30** | The ANAO recommends that organisations clearly specify security aftercare arrangements and promote these arrangements in security education and training activities. |

# Audit Findings and Conclusions

# 1. Introduction

*This chapter provides background information about the audit, including an overview of personnel security requirements. It also describes previous audit coverage of personnel security and explains the approach of the current audit.*

## Personnel security

1.1 Personnel security describes the policies and practices used in managing the risks inherent in allowing Australian government employees and other personnel access to security classified information or resources.

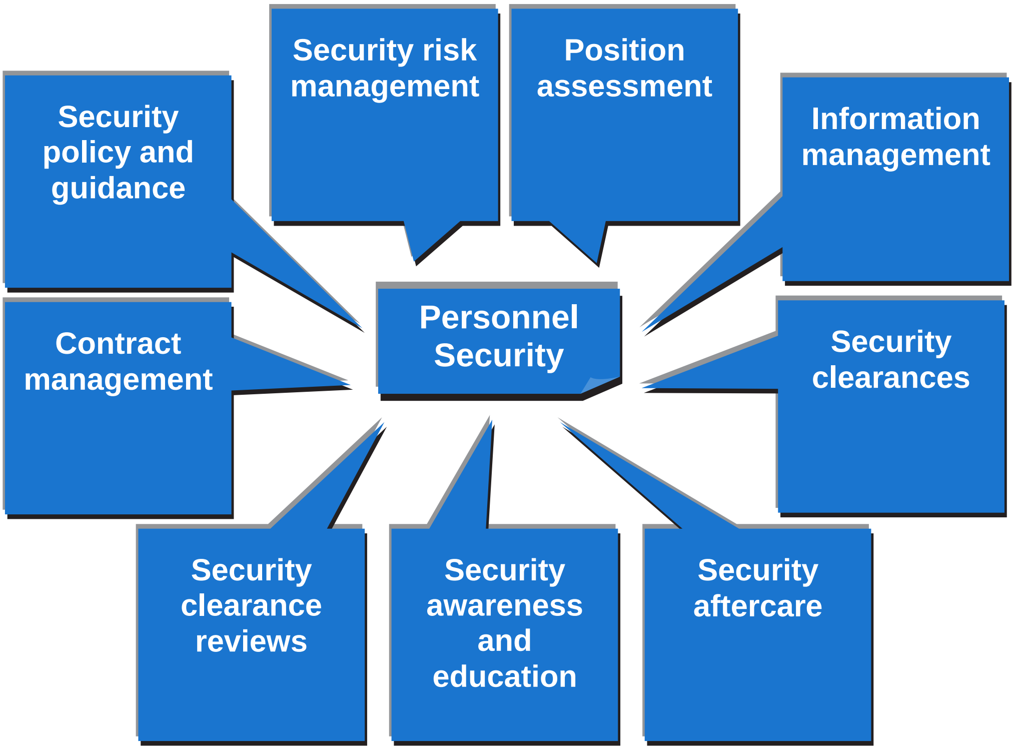
1.2 The central tenet of personnel security is that access to sensitive information is restricted to people with a legitimate requirement, and who are reliable and aware of their responsibilities to protect such information. Consequently, the purpose of the security clearance process is to provide a degree of assurance as to the suitability, trustworthiness, and vulnerability of an organisation's staff.

1.3 There is an increased exposure to security breaches and associated costs and risks if the security clearance process is not conducted objectively and with consideration of key threats and risks.

1.4 Personnel security is an integral part of the framework used by Australian Government organisations to protect official information and resources. As such, effective personnel security requires a comprehensive and coordinated approach that complements other elements of protective security, particularly: physical security; information security, including information and communications technology (ICT) holdings; security in procurement and contracting; and the management of security incidents and investigations. Figure 1.1 illustrates key elements of personnel security.

Figure 1.1

Elements of personnel security



Source: Australian National Audit Office (ANAO).

## The Protective Security Manual

1.5 The Attorney-General's Department (AGD) has overall responsibility for the Australian Government's protective security policy and procedures. The Protective Security Coordination Centre (PSCC) disseminates protective security policy and minimum procedural requirements principally through the Australian Government Protective Security Manual (PSM).[17] The PSM was first published in January 1991 and has been revised and re-released twice, in October 2000 and August 2005.

1.6 Part D of the PSM sets out the policies and standards relating to personnel security, including standards for the conduct and maintenance of

[17] Attorney-General's Department, *Australian Government Protective Security Manual*, Canberra, August 2005. The PSM applies to all agencies subject to the *Financial Management and Accountability Act 1997* (FMA Act), and applies to bodies that are subject to the *Commonwealth Authorities and Companies Act 1997* (CAC Act) which have received notice in accordance with that Act that the Manual applies to them as a general policy of the Australian Government.

security clearances. Part D of the PSM (2005) contains considerably more prescription and guidance than the 2000 version. For example, the number of mandatory minimum standards in Part D increased from 36 in the 2000 version to approximately 120 in the 2005 version.[18]

1.7 AGD advised the ANAO that a review of Australian Government security clearance policy is being undertaken by an inter-departmental committee chaired by the department. The review aims to ensure the policy is relevant to the current security environment and improve the guidance provided to those who conduct security clearance interviews.

1.8 Responsibility for the development, implementation and maintenance of effective personnel security functions lies with the chief executive of each organisation. In many organisations, this responsibility is exercised by a personnel security executive, supported by a security adviser and a team of dedicated security clearance staff.

## Determining security clearance requirements

1.9 According to the PSM, there are two categories of security classified information or resources—national security and non-national security.[19] The PSM describes people requiring access to national security classified information as having a Designated Security Assessment Position (DSAP), and those requiring access to non-national security classified information as being in a Position of Trust (PoT). In this context, a person's eligibility to access security classified information is dependent on:

- a demonstrable 'need to know'—the person will, or may be required to, access security classified information or resources in the course of carrying out their official duties; and
- the conduct of a security clearance—a comprehensive review to confirm the person's identity and assess their suitability to access security classified information.

1.10 The level of security clearance required should be determined by reference to the duties and tasks to be performed, including the security

[18] Appendix 1 of this report illustrates other significant changes in personnel security policy in the 2005 version of the PSM.

[19] National security describes official information which, if compromised, could affect the security of Australia, including its defence systems or operations, international relations or national interests. Non-national security describes official information which, if compromised, does not threaten the security of Australia, but which could threaten the security or interests of individuals, groups, commercial entities, or the safety of the community.

classification of the information that may be accessed. The degree of assurance about the suitability and trustworthiness of staff increases with the level of security clearance, and is based on the security classification of the information to be accessed and the escalating consequences associated with the compromise of that information (see Table 1.1).

### Table 1.1

### Security clearance classification required to access various levels of security-classified information or resources

| Security classification[A] | Impact if information is compromised | Security clearance required |
|---|---|---|
| **National security classification (DSAP)** | | |
| TOP SECRET | Could cause exceptionally grave damage to Australia | TOP SECRET[B] |
| SECRET | Could reasonably be expected to cause serious damage to Australia | SECRET |
| CONFIDENTIAL | Could reasonably be expected to cause damage to Australia | CONFIDENTIAL |
| RESTRICTED | Could possibly be harmful to Australia | Not required |
| **Non-national security classification (PoT)** | | |
| HIGHLY PROTECTED | Could reasonably be expected to cause serious harm to an organisation or individual | HIGHLY PROTECTED |
| PROTECTED | Could reasonably be expected to cause harm to an organisation or individual | PROTECTED |
| IN-CONFIDENCE | Might possibly cause harm to an organisation or individual | Not required |

Notes: (A) Paragraph C6.12 of the PSM describes how to select the appropriate security classification.

(B) There are two categories of TOP SECRET security clearances, known as negative and positive vetting. The basis of negative vetting is that unless the clearance process reveals any information that brings into question the subject's suitability, a security clearance is granted. Positive vetting, on the other hand, requires the suitability of the clearance subject to be established beyond reasonable doubt. The conduct and management of TOP SECRET (positive vetting) security clearances was outside the scope of this audit.

Source: ANAO, based on the PSM.

1.11 As indicated in Table 1.1, a security clearance is not required to access information classified at RESTRICTED or IN-CONFIDENCE levels. In this regard, paragraph D4.8 in the PSM indicates that employment engagement assessments, undertaken in accordance with the requirements of the

*Public Service Act 1999*, are appropriate to allow individuals access to such information.

1.12 Judgements made concerning an individual's eligibility for a security clearance should be subject to ongoing monitoring - for example, to assess if a person has a continuing 'need to know' in relation to security classified information and to identify if any changes in their circumstances have affected their suitability to hold a security clearance.

## Previous audit coverage of personnel security

1.13 Since 2002, three reports have been produced by ANAO and the Joint Committee of Public Accounts and Audit (JCPAA) that assessed the adequacy of personnel security arrangements in Australian Government organisations. As outlined below, these three reports[20] made a total of 14 recommendations for improvement. All recommendations in the two audit reports were agreed by all participating organisations.[21]

### ANAO Audit Report No.22 2001–02, *Personnel Security — Management of Security Clearances*

1.14 In December 2001, the ANAO tabled Audit Report No.22 2001–02, *Personnel Security – Management of Security Clearances*. The objective of the audit was to determine whether organisations were managing security clearance and vetting processes effectively and in accordance with the (then) PSM (2000).

1.15 The audit identified scope to considerably improve a number of aspects of the management, resourcing and operation of personnel security functions. Among the shortcomings were backlogs in the conduct of clearance reviews, a lack of clearance aftercare processes, inadequate security information management and deficiencies in security risk management processes.

1.16 The audit made ten recommendations to assist organisations enhance the effectiveness of their personnel security arrangements, including improving compliance with the requirements of the PSM. Appendix 2 details these recommendations and summarises selected organisations' progress against them.

[20] These three reports are referred to, in some instances, as the previous reports.

[21] Australian Government organisations are not required to provide a formal response as to whether they agree or disagree with recommendations proposed by the JCPAA.

### Review by the Joint Committee of Public Accounts and Audit

1.17 The JCPAA reviewed Audit Report No.22 2001–02 with a particular focus on: security risk assessments; dealing with security clearance backlogs; and the portability of security clearances.[22] The results of the JCPAA's review were published in Report 390, *Review of Auditor General's Reports 2001–02: First, Second and Third Quarters.* That report supported the ANAO's findings and made three additional recommendations. Appendix 2 also details these three recommendations and summarises selected organisation's progress against them.

### Audit Report No.15, 2003–04, *Administration of Staff Employed under the Members of Parliament (Staff) Act 1984*

1.18 In December 2003, the ANAO tabled Audit Report No.15 2003–04 *Administration of Staff Employed under the Members of Parliament (Staff) Act 1984 (MOP(S) Act)*. One of the key objectives of this audit was to review the effectiveness of the internal control structures in the (then) Department of Finance and Administration (Finance) concerning the administration of entitlements for MOP(S) Act staff.

1.19 Among the arrangements reviewed was Finance's administration of the requirement that staff engaged under the terms of the MOP(S) Act obtain (and maintain) a security clearance. Despite noting improvements by Finance in this area, the audit reported that 18 per cent of ministerial staff did not have a current security clearance. Accordingly, it recommended that Finance improve processes to encourage MOP(S) Act staff to gain security clearances (see Appendix 2).

## Current audit

1.20 Due to the significance of the shortcomings identified, and the number of recommendations made, in the previous ANAO audits and JCPAA inquiry, the ANAO has undertaken this follow-up audit.

### Audit objective, criteria and scope

1.21 The objective of this audit is to assess the effectiveness of personnel security arrangements at selected Australian Government organisations, including whether they satisfied the requirements of the PSM.

[22] Portability describes the principle that security clearances conducted in accordance with the minimum requirements in the PSM should be recognised by all Australian Government organisations.

1.22 To address this objective the audit examined the extent to which the selected organisations had implemented:

- all 10 recommendations in Audit Report No.22 2001–02, *Personnel Security—Management of Security Clearances;*
- Recommendations No. 7, 8 and 9 in JCPAA Report 390, *Review of Auditor-General's Reports 2001–02, First, Second and Third Quarters*; and
- Recommendation No. 1 in Audit Report No.15 2003–04, *Administration of Staff Employed Under the Members of Parliament (Staff) Act 1984*.

1.23 These recommendations represent the audit criteria. The audit scope also takes into account the update of the PSM from the 2000 version applying at the time of the previous audit to the current version released in August 2005.

## Audit coverage and methodology

1.24 Personnel security arrangements at four Australian Government organisations were assessed against all ten recommendations from ANAO Audit Report No.22 and two of the additional recommendations from JCPAA Report 390.[23] These four organisations were:

- Australian Prudential Regulation Authority (APRA);
- Commonwealth Scientific and Industrial Research Organisation (CSIRO);
- Department of Defence (Defence); and
- Department of Immigration and Citizenship (DIAC).

1.25 These four organisations processed around 39 000 clearances between January 2005 and November 2007 and, in total, had approximately 125 000 active security clearances.[24] These organisations granted security clearances to over 99 per cent of all individuals requiring clearances between January 2005 and November 2007.[25]

[23] The two relevant recommendations were Recommendation No. 7, regarding the level of resources allocated to the conduct and administration of security clearances, and Recommendation No. 8 regarding the management of personnel security information.

[24] One organisation had approximately 90 per cent of this total.

[25] Rather than deny a clearance, organisations can adequately protect information through more moderate approaches, such as granting the security clearance subject to conditions, downgrading the clearance to a lower level or changing the duties of the individual to avoid the need for a security clearance.

1.26 For these four organisations, the audit methodology included interviews with key staff and a review of relevant documentation including policy and related guidance material, security risk assessments, security awareness and training programs, and management reports outlining personnel security performance. The ANAO also examined a sample of security clearances granted by the four organisations between January 2005 and November 2007.

1.27 The audit also assessed the extent to which:

- AGD had implemented Recommendation No. 9 in JCPAA Report 390, which proposed that AGD report on the cost-effectiveness of maintaining a central database of security clearances; and
- Finance had implemented Recommendation No. 1 from ANAO Audit Report No.15 2003–04, regarding security clearances for MOP(S) Act staff.

1.28 Following the conduct of fieldwork, each of the six selected organisations was provided with a management report setting out the scope of work undertaken and detailing the audit findings, conclusions, and where appropriate, recommendations for improvement.

## Assistance to the audit

1.29 The ANAO engaged Allanson Consulting to provide a range of statistical analysis for the audit.

1.30 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately $415 000.

## Audit reporting and structure

### Background to protective security audits

1.31 Following a recommendation from the 1979 *Inquiry into Protective Security*, undertaken by Mr Justice Hope, the ANAO commenced a program of audits to evaluate protective security arrangements in Australian Government organisations. In the majority of cases, these audits were conducted and reported on an individual organisation basis (that is, independently from each other). In 1995, the ANAO included protective security audits in its cross-agency general performance audit program, which is undertaken pursuant to section 18 of the *Auditor-General Act 1997.* This section provides that the ANAO may examine a particular aspect of the operations of the whole, or of a part of the Australian Government sector.

1.32 This is the ninth cross-agency protective security audit conducted by the ANAO under these arrangements. Appendix 3 lists the earlier protective security audits undertaken by the ANAO. The audit recommendations in protective security audit reports are framed to have general application and the audit findings are reported to Parliament in generic terms, without being attributed to particular organisations. Where appropriate, this report also includes references to sound and better practices identified during the audit.

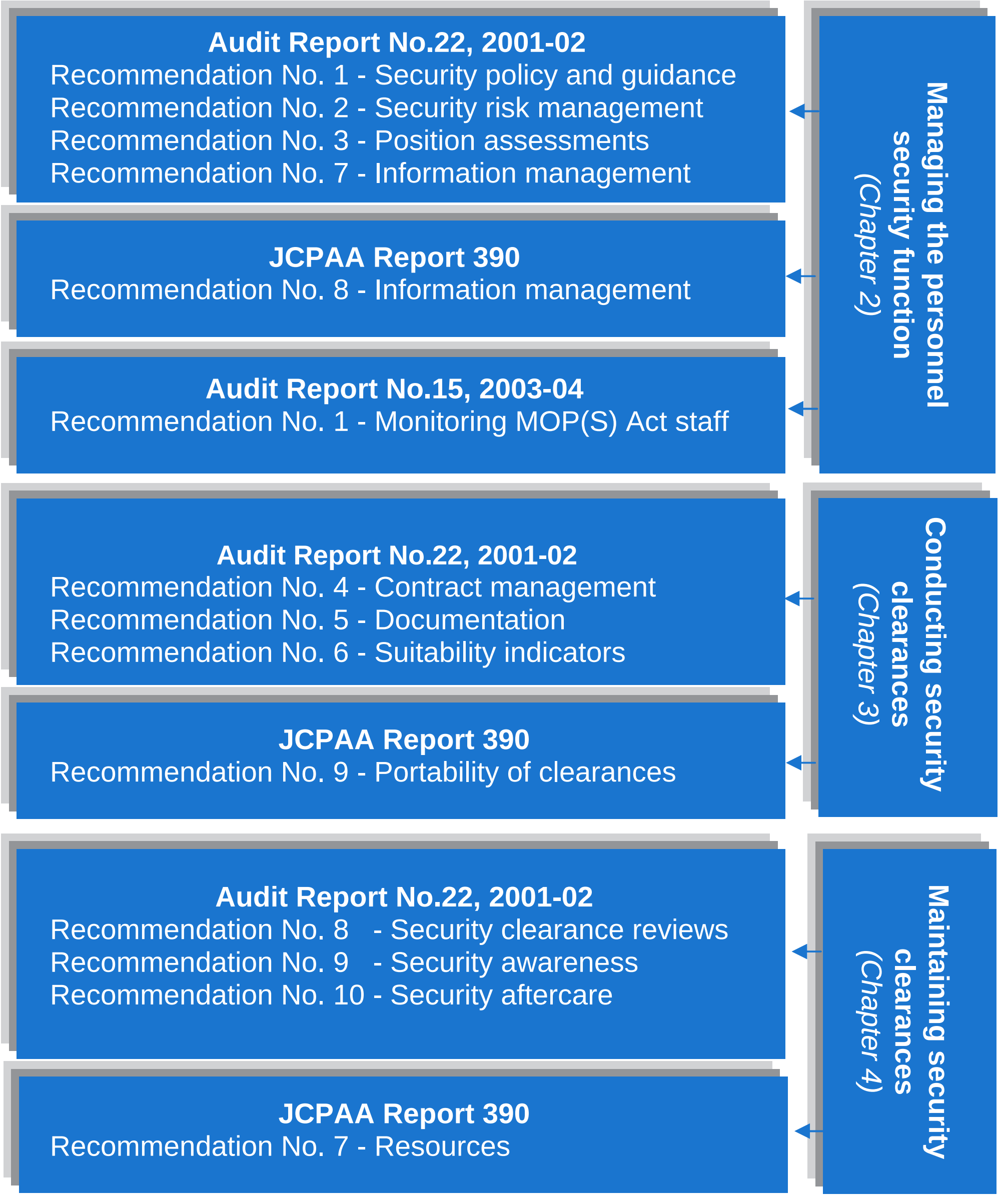
## Audit structure

1.33 For the purposes of this audit, the 14 recommendations being examined have been grouped into three broad themes—managing the personnel security function, and conducting and maintaining security clearances. Each of these recommendations is discussed in more detail, together with an analysis of progress made by the selected organisations in implementing the recommendations, in Chapters 2 to 4 (see Figure 1.2). The report also contains four appendices:

- Appendix 1 illustrates significant changes in personnel security policy in the 2005 version of the PSM;
- Appendix 2 details recommendations from the three previous reports, and summarises selected organisations' progress against them;
- Appendix 3 lists protective security audits undertaken by the ANAO; and
- Appendix 4 provides a schedule of sub-criteria used in the ANAO's examination of security clearances.

**Figure 1.2**

**Grouping of recommendations from previous reports into audit themes**



**Audit Report No.22, 2001-02**
Recommendation No. 1 - Security policy and guidance
Recommendation No. 2 - Security risk management
Recommendation No. 3 - Position assessments
Recommendation No. 7 - Information management

**JCPAA Report 390**
Recommendation No. 8 - Information management

**Audit Report No.15, 2003-04**
Recommendation No. 1 - Monitoring MOP(S) Act staff

**Managing the personnel security function** *(Chapter 2)*

**Audit Report No.22, 2001-02**
Recommendation No. 4 - Contract management
Recommendation No. 5 - Documentation
Recommendation No. 6 - Suitability indicators

**JCPAA Report 390**
Recommendation No. 9 - Portability of clearances

**Conducting security clearances** *(Chapter 3)*

**Audit Report No.22, 2001-02**
Recommendation No. 8 - Security clearance reviews
Recommendation No. 9 - Security awareness
Recommendation No. 10 - Security aftercare

**JCPAA Report 390**
Recommendation No. 7 - Resources

**Maintaining security clearances** *(Chapter 4)*

Source: ANAO.

# 2. Managing the Personnel Security Function

*This chapter addresses the implementation of those recommendations from the previous reports that were designed to improve the management and control of personnel security functions.*

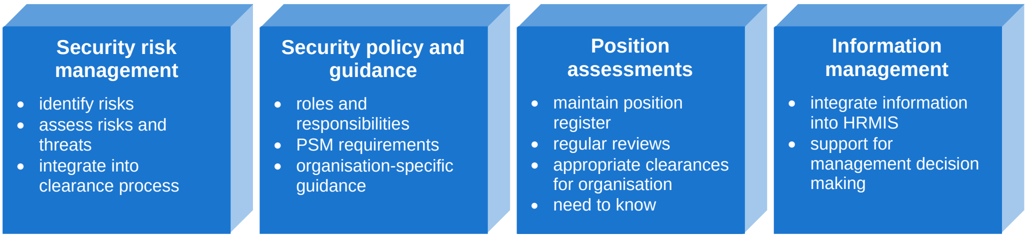
## Introduction

2.1 A mature framework for managing personnel security incorporates minimum requirements outlined in the PSM into an organisation's broader security operations, with links to the control environment.[26]

2.2 Key factors underpinning the effective management of personnel security functions include: comprehensive policy and guidance material; an understanding of potential risks and threats; identifying and monitoring security clearance requirements; and access to accurate and current information to support decision-making (see Figure 2.1).

### Figure 2.1

**Managing the personnel security function**


Security risk management
• identify risks
• assess risks and threats
• integrate into clearance process
Security policy and guidance
• roles and responsibilities
• PSM requirements
• organisation-specific guidance
Position assessments
• maintain position register
• regular reviews
• appropriate clearances for organisation
• need to know
Information management
• integrate information into HRMIS
• support for management decision making

Source: ANAO.

2.3 In this context, the ANAO examined the extent to which the selected organisations implemented the following recommendations:

- Audit Report No.22 2001–02, Recommendation No. 1, 2, 3 and 7;
- Audit Report No.15 2003–04, Recommendation No. 1; and
- JCPAA Report 390, Recommendation No. 8.

[26] The control framework provides an important link between an organisation's objectives and the functions and tasks to achieve these objectives.

## Security policy and guidance

2.4 Well-designed personnel security policy and procedural documentation is a key source of information and instruction for staff in the performance of their respective roles and responsibilities. A lack of effective policy and guidance documentation can increase the risk of:

- variations in the depth of awareness and understanding about organisational and Australian Government standards;
- inconsistent practices occurring; and
- inadvertent non-compliance with the personnel security requirements of the PSM .

### Findings of the previous audit

2.5 Audit Report No.22 2001–02 identified several shortcomings in personnel security policy and procedural documentation amongst the audited organisations. For example, some of the policy and procedural documentation reviewed largely consisted of extracts from, or reference to, the PSM. In these cases, there was little organisation-specific guidance material.

Audit Report No.22 2001–02, Recommendation No. 1

The ANAO recommends organisations approve and promulgate appropriate policy and procedures to support the conduct and administration of personnel security. In this regard, policy and procedures should be based on, but not necessarily limited to, the policy and guidance material contained in PSM (2000).[27]

### Findings of the current audit

The selected organisations had personnel security policies and procedural documentation of varying detail and usefulness, but had generally not specifically reviewed all of this material in light of the revised PSM in 2005.

*One* of the selected organisations had *fully* implemented this recommendation, *two* organisations had *substantially* implemented it, and the *other* had *partially* implemented it.

2.6 Each of the selected organisations had promulgated a series of policy and procedural documents relating to their personnel security functions. This material varied in detail and usefulness between organisations, but for the

[27] ANAO Audit Report No.22 2001–02, op. cit., p. 36.

most part was informative and helpful to staff. Personnel security policy and procedural material was contained on each organisation's intranet.

2.7 To complement policy documentation, two organisations had developed a series of detailed guidelines dealing with the conduct and management of security clearances. In both cases, the ANAO considered that the guidelines set out and comprehensively explained the standards and practices required to implement their respective policies. As well as referring to relevant minimum requirements of the PSM (2005), both sets of guidelines also addressed a range of organisation-specific issues.

2.8 The main shortcoming observed during the audit was that no organisation had systematically assessed the appropriateness of each of their policy, procedural or guidance documentation in light of the release of the revised PSM in 2005. At the time of the audit, three organisations had initiated but not completed such reviews.

2.9 The ANAO suggests that organisations assess, at least annually, the continued appropriateness of personnel security policies, including whether they reflect the organisation's operating environment, and are consistent with principles and requirements contained in the PSM.

## Security risk management

2.10 The design of an organisation's protective security processes and controls should be informed by an assessment of pertinent risks or threats. In the personnel security context, the identification and analysis of risks could contribute to improved personnel security by highlighting, for example:

- factors requiring additional or supplementary checks to be undertaken as part of the security clearance process;
- matters to include in security awareness briefings and training programs; or
- criteria used to initiate the review of a security clearance.

### Findings of the previous audit

2.11 None of the organisations involved in Audit Report No.22 2001–02 had fully assessed how security risk factors might be reflected in, or used to inform personnel security practices, including the conduct of security clearances.

Audit Report No.22 2001–02, Recommendation No. 2

The ANAO recommends organisations review their security risk management processes against the requirements of Part B of PSM 2000 and, in particular, ensure:

- personnel security threats and hazards are thoroughly considered in this process; and
- organisation-specific security risks are factored into the security clearance process, as appropriate.[28]

## Findings of the current audit

One organisation had demonstrated a mature risk-based approach to managing personnel security. Conversely, three organisations did not have an up-to-date record of their personnel security risks, including one which did not have systematic processes for managing these risks.

*One* organisation had *fully* implemented this recommendation, *two* had *partially* implemented it, and the *other* had *not* implemented it.

2.12 Three organisations had policies and processes in place to identify, assess and manage security risks.

2.13 However, the ANAO considered that only one organisation had an adequate record of risks, and associated risk-mitigation controls, involved in the delivery of its personnel security functions. In 2007, that organisation undertook a systematic review of potential threats across each dimension of protective security. More specifically, the review assessed the potential impact of a range of risks on its personnel security functions, including the conduct of security clearances. The organisation had formulated a security plan, which amongst other things, contained:

- a schedule of risk treatments;
- the identity of the official responsible for implementing each treatment; and
- details of monitoring arrangements.

2.14 At the time of the audit, the organisation had made substantial progress in implementing the process improvements identified during the security risk assessment.

[28] ibid., p. 37.

**2.15** One organisation had not formally reviewed the risks, and associated controls, it had identified in a security risk assessment undertaken early in 2005. In the absence of such an assessment, there was considerable uncertainty as to whether the organisation was properly informed about new or emerging risks. In addition, changing circumstances cast doubt on the continuing effectiveness of controls identified to manage the originally assessed risks.

**2.16** Another organisation did not have a current risk assessment for its personnel security operation. It did, however, have a robust framework for the conduct of security risk assessments, including formally recognising the principles relating to risk management contained in Part B of the PSM (2005).

**2.17** At the time of the audit, the remaining organisation had not assessed, and did not have a framework for managing, security risks.

**2.18** Having current information about security risks contributes to the effective control and management of an organisation's personnel security function. In the absence of current assessments, organisations are unlikely to effectively manage risks to their personnel security functions, including ensuring that organisation-specific risks are appropriately factored into security clearance processes.

## Recommendation No.1

**2.19** The ANAO recommends that organisations regularly review personnel security risk assessments to identify new or emerging risks or changes in risk ratings, and assess the effectiveness of risk treatments.

### Organisations' responses to the recommendation

**2.20** Each of the audited organisations agreed with the recommendation.

## Position assessments

**2.21** Security clearances should only be undertaken for people assessed as requiring access to security classified information or resources to carry-out their official duties. This is commonly described as conducting a 'position assessment'. The effective management of position assessments, including monitoring their continued appropriateness, can contribute to better utilisation of personnel security resources.

## Findings of the previous audit

2.22 Audit Report No.22 2001–02 identified several shortcomings in the management of position assessments. For example, the audit found:

- line managers often requested security clearances without sufficient consideration of the need for a security clearance;
- a lack of guidance to assist staff making assessments; and
- processes for the ongoing or periodic review of existing position assessments were ineffective.

Audit Report No.22 2001–02, Recommendation No. 3

The ANAO recommends:

- registers of Designated Security Assessment Position (DSAP) and Positions of Trust (PoT) are reviewed periodically to ensure they accurately reflect the organisation's continued security clearance requirements; and
- organisations develop appropriate guidelines to assist managers to undertake position assessments.[29]

## Findings of the current audit

All four organisations had identified, recorded and maintained security clearance requirements for each position to varying degrees. In this regard, two organisations had fully-documented, systematic approaches, while one organisation mainly relied on a case-by-case approach. At the other organisation, a large proportion of security clearance requirements were driven by decisions to require a minimum level of clearance for certain staff.

*One* organisation had *fully* implemented this recommendation, two had *substantially* implemented it, and one had *partially implemented* it.

2.23 Two organisations had systematic processes for identifying, recording and maintaining security clearance requirements for each of the positions in their establishments. At both of these organisations, information obtained from these processes provided the basis for, and was used in, the conduct of security clearances. Both of these organisations also had clear policies outlining the maintenance of position assessment information.

[29] ibid., p. 38.

2.24 In an example of a better practice, one organisation utilised its Human Resource Management Information System (HRMIS) to record, approve and monitor the currency of security clearance requirements for each position. The ANAO considered this approach better facilitated effective management of, and decision-making about, the organisation's security clearance requirements. In particular, the inclusion of this information in the HRMIS:

- improved the ability of the personnel security unit to monitor the appropriateness of security clearance requirements for each position;
- enabled the capture of changes to these requirements in a timely manner; and
- provided a reliable basis for identifying discrepancies between security clearance requirements and actual security clearance levels.

2.25 During 2007, this organisation conducted an organisation-wide review of position assessment information. This review assessed the continued appropriateness of security clearance requirements recorded in the HRMIS (in terms of the work performed by the occupant of each position) and, as necessary, updated those details.

2.26 In the other organisation with clear policies regarding the maintenance of position assessment information, the assessment of security clearance requirements (and the management of position assessment information) was the responsibility of individual work-areas or units. Although the organisation's centralised personnel security team captured details of individual position assessments during the 'request for security clearance' process, it did not have any regular oversight of position assessment records. In addition, it did not have programs to systematically evaluate the accuracy and completeness of these records.

2.27 One organisation advised the ANAO that much of its security clearance requirements were determined by decisions to require a minimum of SECRET level clearances for certain categories of staff. In other cases at this organisation, the need for, and the level of, security clearances is generally determined on a case-by-case basis, depending on the clearance subject's duties and responsibilities.

2.28 In the remaining organisation, the need for security clearances was largely determined on a case-by-case basis depending on an individual's duties.

2.29 An accurate record of security clearance requirements is an important element in the management of personnel security. In particular, it can assist organisations identify, and take action on, any discrepancies between security clearance requirements and the actual number and level of security clearances.

## Information management

2.30 Access to a range of timely and accurate information is an important element in effective personnel security decision-making. The ANAO considers that greater reliance on automation, such as specialist personnel security databases or the organisation's HRMIS, is central to the effective management of personnel security information. The inclusion of personnel security information in the HRMIS is generally considered to be better practice. However, decisions to integrate existing systems must consider whether it is cost-effective to do so.

### Findings of the previous audit and the JCPAA report

2.31 Only two of the organisations involved in Audit Report No.22 2001–02 had integrated personnel security information into their HRMIS. The other four organisations used a range of standalone applications or other limited solutions.

Audit Report No.22 2001–02, Recommendation No. 7

To improve the effectiveness of security information management, the ANAO recommends organisations assess opportunities to integrate the management of personnel (including contractor) security information into the organisation's HRMIS or other appropriate corporate system.[30]

2.32 The JCPAA endorsed the ANAO's finding on this matter. In Report 390, the Committee noted that many organisations did not have adequate information management systems to support their security clearance processes and that this impacted upon their ability to manage these processes.

JCPAA Report 390, Recommendation No. 8

The JCPAA recommends all organisations make the necessary changes to their HRMIS to support management reporting in relation to security clearances and appropriate access to security clearance information.[31]

[30] ibid., p. 53.

[31] JCPAA Report 390, p. 59.

## Findings of the current audit

Two organisations either integrated personnel security information with, or had adequate links to relevant information in, a HRMIS, while two organisations did not use a HRMIS. Of the two that had not, one organisation had commenced a program to provide adequate integration, and the other had so few clearances that integration was not warranted.

*Two* organisations had *fully* implemented ANAO Report No.22 2001–02, Recommendation No. 7, *one* had *substantially* implemented it and *one* had *partially* implemented it.

*Two* organisations had *fully* implemented JCPAA Report 390, Recommendation No. 8, *one* had *not* implemented it, and it *did not apply* to the *other*.

### *Arrangements for recording personnel security information*

2.33 The selected organisations used a variety of approaches to record personnel security information, including details of security clearances.

2.34 However only one organisation had integrated personnel security information, as well as details of position assessments, into its HRMIS. The ANAO considers that the integration of personnel security information into the HRMIS is an example of better practice. The approach enhances the ability of the organisation to monitor the currency of personnel security records, including capturing any changes relating to clearances. In this case, the inclusion of personnel security information in the HRMIS also facilitated better integration and alignment between the organisation's personnel security and recruitment functions.

2.35 Two of the selected organisations held security clearance details in specialised personnel security management systems. Both organisations advised that integration of security clearance information into their respective HRMIS was not practicable, nor cost-effective. The personnel security management system at one of these organisations contained a link to number of information fields in the organisation's HRMIS. This link enabled the personnel security business unit to identify relevant information from the HMRIS in a timely manner, for example, details of staff movements and terminations.

2.36 The remaining organisation maintained details of security clearances in its records management system (which records details of personal security files) and also in a spreadsheet. Given the small number of clearances at this organisation, the audit considered these arrangements to be appropriate.

Reviewing arrangements for recording personnel security information

2.37 At the time of the audit, two organisations had proposals to further enhance processes to record personnel security information. Of these:

- one organisation indicated it would examine opportunities to integrate personnel security information into its new management information system; and
- one organisation planned to upgrade its personnel security management information system to enable the electronic submission, transfer, processing and management of security clearance forms.

*Monitoring and reporting personnel security performance*

2.38 Only two organisations actively monitored information on the performance of the personnel security function, including security clearance workload. In both cases, details of performance were regularly provided to senior executives.

2.39 One organisation included statistics on security clearance workload (on-hand and completed), as well as attendance at security training, in a 'Security Health' report each month. That organisation also reported details of vetting caseload (by clearance level), including the number of new and finalised cases, to relevant managers each week.

2.40 The other organisation distributed monthly and quarterly reports on vetting performance, including a range of workload statistics by clearance level, an analysis of the trends in those statistics and details of emerging issues. These performance reports also separately address initial clearance and clearance review performance.

2.41 The ANAO suggests that organisations regularly capture and report information on personnel security performance, including information on the conduct of security clearances. In addition, if they have not already done so, organisations should also evaluate the cost-effectiveness of integrating personnel security information into the HRMIS to better support performance management.

## Monitoring security clearances of MOP(S) Act staff

2.42 Under the provisions of the MOP(S) Act, the employment of staff by Australian Government Ministers and Parliamentary Secretaries is conditional upon the employee obtaining and maintaining a TOP SECRET security clearance.[32] Finance is responsible for supporting staff employed under the MOP(S) Act. Finance provides a range of support services to parliamentarians and their staff, including facilitating security clearances for ministerial staff. The department's responsibilities in relation to security clearances are set out in the Ministers of State Entitlements Handbook.

**2.43** Finance does not have the authority to compel MOP(S) Act staff to comply with the requirement for a security clearance. As such, Finance remains dependant on ministerial support to help ensure compliance of MOP(S) Act with security clearance requirements.

## Findings of the previous audit

**2.44** Audit Report No.15 2003–04 reported that in June 2002, 215 ministerial staff (44 per cent) did not have a current security clearance. However, by October 2003, the number of outstanding clearances had been reduced to 88 (18 per cent).

**Audit Report No.15 2003–04, Recommendation No. 1**

The ANAO recommends Finance strengthen monitoring procedures to ensure MOP(S) Act staff with outstanding security clearances are identified in a timely manner, and that appropriate follow-up is undertaken with relevant staff members, their employing Parliamentarians and the security-vetting agency undertaking the security clearances.[33]

## Findings of the current audit

Since the previous audit, Finance enhanced its administration of security clearances for MOP(S) Act staff, and implemented this recommendation.

**2.45** Key initiatives taken by Finance to enhance the administration of security clearances for MOP(S) Act staff include:

- increasing resources allocated to the function;
- developing a set of procedures which, amongst other things, outline the records and other references required to fulfil the function;

[32] This requirement is communicated in: Determination 2004–05/Part III/6 under subsection 14(3) of the MOP(S) Act; the terms and conditions of employment for Office Holders (under Part III of the MOP(S) Act); letters of appointment for Ministerial/Parliamentary Secretary staff; the Ministers of State Entitlements Handbook; and the Prime Minister's *A guide to key elements of Ministerial Responsibility* (Part 9 – Ministerial Staff Conduct).

[33] ANAO Audit Report No.15 2003–04, op. cit., p. 56.

- improving the measurement and reporting of performance, including regularly providing workload statistics to the Special Minister of State, as well as advice on the status of relevant security clearances, to other key stakeholders;
- adopting more structured processes for following-up outstanding clearance packs, including introducing a formal non-compliance process for those staff who do not submit the necessary forms within a pre-determined time period;
- engaging a second vetting service provider to conduct security clearances; and
- identifying clearances due for re-validation or re-evaluation in advance.

**2.46** Finance's formal non-compliance process was an important initiative to improve MOP(S) Act staff compliance with personnel security requirements. This process was introduced in October 2007 and established a timeframe of 12 weeks for MOP(S) Act staff to submit their completed security clearance packs. If packs are not provided within that period, Finance commences a clearance denial process. The process had been invoked in a number of instances by June 2008, and was effective in following-up staff with outstanding security clearance packs. The ANAO notes that the overall effectiveness of the process is likely to become more apparent in coming months, as decisions are made about its application to many more MOP(S) Act staff who currently have not submitted completed security clearance packs within 12 weeks of receiving them

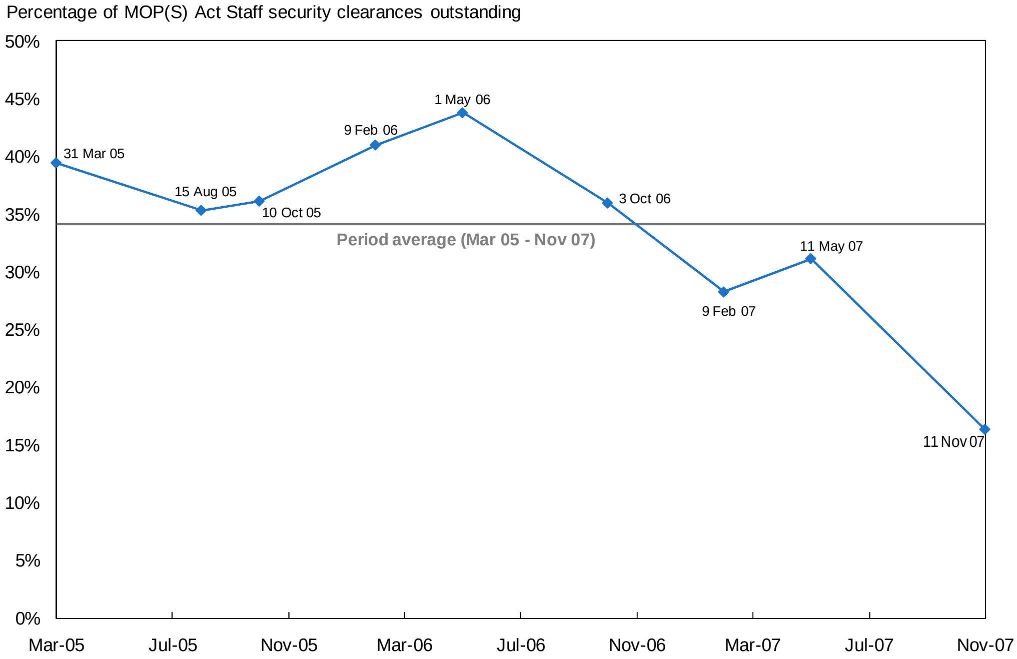
**2.47** As shown in Figure 2.2, there has been a significant reduction in the proportion of security clearances for MOP(S) Act staff that were outstanding[34] since May 2006. As at November 2007, 16 per cent of MOP(S) clearances were outstanding. This is less than half the average over the period March 2005 to November 2007,[35] and was slightly lower than the level at October 2003 (18 per cent) that was reported in the previous audit. The ANAO considers that this result reflects improvements made by Finance in the administration of security clearances for MOP(S) Act staff.

[34] Outstanding security clearances are those in progress or overdue. Security clearances in progress are those where the clearance subject had returned a completed security pack enabling the assessment process to commence, but it has not been completed. Overdue clearances are those where the subject has not returned a completed security pack and the assessment process had not commenced.

[35] Data was readily available for this period. Further, Finance advised that the peak proportion of outstanding security clearances in this period (45 per cent in May 2006) was predominantly due to delays occurring at its contracted service provider.

## Figure 2.2

### *Proportion of MOP(S) Act staff clearances that are outstanding over the period March 2005 to November 2007*



Source: ANAO, based on statistics maintained by Finance.

2.48 As a result of the change of government following the Federal election held on 24 November 2007, security clearances for MOP(S) Act staff employed by the previous government were suspended by Finance. Finance has commenced processing security clearances for the staff of the new government. The ANAO recognises that this is likely to create a short-term increase in workload and also impact on the timeliness of clearance processing by the contracted security clearance providers.

# 3. Conducting Security Clearances

*This chapter addresses the implementation of those recommendations from the previous reports that were designed to improve processes for the conduct of security clearances, including to meet the requirements of the PSM.*

## Introduction

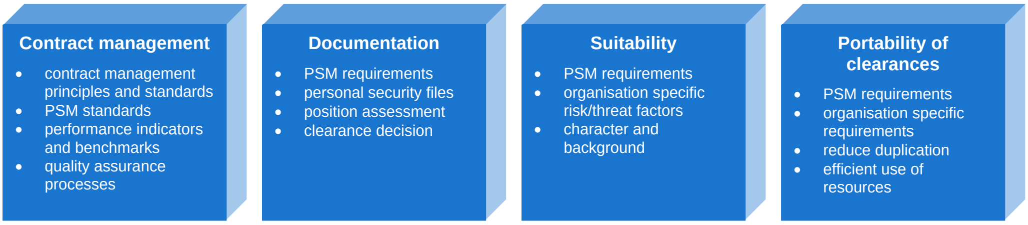
3.1 Australian Government organisations use in-house resources, engage external service providers, or utilise some combination of the two, to conduct security clearances. While the responsibility to perform services may be transferred to an external service provider, accountability for security arrangements remains with the organisation. Consequently, each organisation is required to ensure that security clearances are undertaken in accordance with the minimum standards in Part D of the PSM (2005), irrespective of whether security clearances are undertaken within the organisation or by contractors.

3.2 The security clearance process is designed to assess whether individuals with access to classified or sensitive information can be relied upon to properly use and protect that information. In conducting a security clearance, the organisation must obtain and evaluate sufficient information to be reasonably assured of the individual's responsibility, integrity and maturity, in light of the individual's prospective position and the organisation's risk and threat environment.

3.3 Figure 3.1 illustrates the major elements in conducting a security clearance that are considered in this chapter.

### Figure 3.1

**Conducting a security clearance**



**Contract management**

- contract management principles and standards
- PSM standards
- performance indicators and benchmarks
- quality assurance processes

**Documentation**

- PSM requirements
- personal security files
- position assessment
- clearance decision

**Suitability**

- PSM requirements
- organisation specific risk/threat factors
- character and background

**Portability of clearances**

- PSM requirements
- organisation specific requirements
- reduce duplication
- efficient use of resources

Source: ANAO.

3.4 Specifically, the ANAO has examined the extent to which the selected organisations have implemented the following recommendations:

- Audit Report No.22 2001–02, Recommendation No. 4, 5 and 6; and
- JCPAA Report 390, Recommendation No. 9.

## Contract management

3.5 The PSM (Part F) sets out the principles and standards for minimising security risks involved in procurement and contracting. Among the requirements of the PSM are that Australian Government organisations actively manage contracted service providers by regularly monitoring their performance, including adherence to relevant security standards. This is also a key principle outlined in the ANAO's *Better Practice Guide: Developing and Managing Contracts*.[36]

3.6 To exhibit features consistent with the PSM and the ANAO guide, contracts for processing personnel security clearances should include:

- clear quality and performance measures;
- standards relating to information security;
- turnaround times (including provision for complex cases);
- organisation-specific risk factors; and
- quality assurance mechanisms, including periodic review.[37]

### Findings of the previous audit

3.7 ANAO Audit Report No.22 2001–02 found that the selected organisations generally had insufficient processes to manage the performance of contracted service providers. The key findings from that audit were that:

- standards of performance were not clearly defined;
- organisations had not conducted reviews of the services delivered under contract;

[36] ANAO, *Better Practice Guide: Developing and Managing Contracts – Getting the Right Outcome, Paying the Right Price*, February 2007.

[37] ANAO Audit Report No.22 2001–02, op. cit., p. 38.

- there was a lack of quality assurance processes to assess the appropriateness and reliability of security clearance recommendations made by contracted service providers; and
- there was a lack of organisation-specific risk factors and details of organisation-specific security clearance requirements in contracts or agreements.

Audit Report No.22 2001–02, Recommendation No. 4

The ANAO recommends organisations adopt better practice contract management principles and standards in outsourced security clearance and vetting service arrangements.[38]

## Findings of the current audit

The three organisations with outsourced arrangements had effectively managed the workload and timeliness of external providers conducting security clearances but had not explicitly measured the quality of assessments they had undertaken.

*All three* organisations had *substantially* implemented this recommendation.

3.8 Two selected organisations outsourced the conduct of all security clearances to external providers, another organisation outsourced around 35 per cent of its annual workload of security clearances, while the remaining organisation conducted all of its security clearances in-house.

3.9 The contracts in two selected organisations were generally well structured and provided coverage of most of the factors necessary to support effective contract management. For example, the contracts: identified the required standards of work; dealt with information security; included details of organisation-specific risk factors; and required the adherence to organisation-specific policies, forms and guidelines.

3.10 The major shortcoming in the design of the contracts was that they lacked information on measuring the performance of contractors, including identifying specific performance indicators. The only performance indicator included in the contracts examined related to timeframes for completing the prescribed tasks.

3.11 Other relevant indicators of performance relate to quality and could include: adherence to the organisation's policies and standards; the level of appropriateness and completeness of security clearance assessments; evidence

[38] ibid., p. 38.

of checking or review; and adherence to the requirements of the PSM. In this regard, while some contracts indicated that the services were to be conducted in accordance with the requirements of the PSM, they did not detail these requirements.

3.12 Given the potential risks involved, sound management of work performed by contracted service providers is vital to help ensure that they operate at a consistently high standard and in accordance with the minimum standards of the PSM. In this regard, the selected organisations had a range of mechanisms to assist in the ongoing management of work being outsourced. These arrangements included:

- the use of a checklist to: assess whether clearances were being completed within allocated timeframes; identify reasons for any delays outside the contractor's control; and recommend whether payment should be withheld;
- a program of monthly meetings with the contracted service providers to discuss workload and performance issues;
- six monthly meetings with the contracted service providers to deal with broader strategic issues;
- capturing information on security clearance completion rates each month (to provide a basis for the allocation of work);
- checking work done by contracted service providers prior to granting (or denying) the clearance; and
- undertaking formal quality assurance reviews of a sample of the security clearances done by contracted service providers.

3.13 Notwithstanding the lack of systematic measurement of quality, testing for this audit found that contracted service providers typically conducted security clearance assessments to a high standard, as reflected in comprehensive documentation contained on personal security files.

## Documentation

3.14 Information recorded on an individual's personal security file should be sufficient to fully justify the decision to grant or deny a security clearance. In this regard, the personal security file should include: details of the position assessment; copies of all relevant personal documentation (properly certified);

interview and referee reports (where these are required); a record of the checks and enquiries undertaken; and a copy of the clearance decision.

## Findings of the previous audit

3.15 Audit Report No.22 2001–02 found that documentation contained on personal security files was, for the most part, sufficient and appropriate to support the clearance decision. However, some weaknesses were observed and these included:

- some personal security files only contained copies of handwritten interview notes, rather than more formal interview reports, setting out the assessing officer's analysis and conclusions;
- some files lacked evidence that the checks required by the PSM had been undertaken; and
- a number of referee's reports were considered to be of only limited use because they were too generic and had not addressed factors relevant to security, including the subject's suitability for a security clearance.

Audit Report No.22 2001–02, Recommendation No. 5

The ANAO recommends organisations record all information collected during the course of a security clearance on the individual's personal security file.[39]

## Findings of the current audit

Three of the four organisations had recorded sufficient information on the subject's personal security file to fully justify the decision to grant a security clearance.

*Three* organisations had *fully* implemented this recommendation and the *other* had *partially* implemented it.

3.16 The ANAO examined security clearances granted between January 2005 and November 2007 at four organisations. At three of the organisations, the ANAO examined a stratified random sample of the security clearances granted in this period.[40] At the remaining organisation, given the small number of clearances, the ANAO examined all the security clearance files.

[39] ibid., p. 46.

[40] The sample was stratified to ensure adequate coverage of the different levels of security clearances in each organisation.

3.17 Details of the number of security clearances granted during the relevant period (by level) and the number of clearances examined by the ANAO are shown in Table 3.1.

### Table 3.1

### Security clearances examined during this audit

| Classification | Number of clearances granted | Number of clearances examined by ANAO |
|---|---|---|
| TOP SECRET | 10 255 | 153 |
| SECRET | 21 974 | 209 |
| CONFIDENTIAL | 2 954 | 67 |
| HIGHLY PROTECTED | 208 | 61 |
| PROTECTED | 4 361 | 90 |
| TOTAL | 39 752 | 580 |

Source: ANAO, based on information at the selected organisations.

3.18 A total of seven security clearances initially selected for examination in two of the organisations were unable to be tested as the individual's personal security file could not be located. These missing files contain a range of sensitive personal information and represent a serious breakdown in recordkeeping practices.

3.19 The accuracy and completeness of the information collected for each of the examined security clearance was evaluated against the five criteria shown in Table 3.2.[41] The criteria were based on requirements in Part D of the PSM (2005).

[41] Each of these criteria comprised a number of sub-criteria. These sub-criteria are outlined in Appendix 4.

## Table 3.2

### Criteria used to evaluate security clearances

| Criteria | Evidenced by the subject's personal security file containing… |
|---|---|
| Security clearance request | a formal and approved request to conduct a security clearance *(PSM, paragraph D7.5).* |
| Information forms and consents | a series of forms and consents completed by the clearance subject (*PSM, paragraphs D7.23/34*). |
| Mandatory personal documentation | certified copies of the personal documents or certificates required to confirm the identity of the clearance subject (*PSM, paragraphs D7.40/42).* |
| Checks and inquiries | a range of checks and inquiries in order to establish the clearance subjects suitability to hold a security clearance (*PSM, paragraphs D6.38, D7.29 and D7.83/98).* |
| Clearance decision | a copy of the advice of the clearance decision (*PSM, paragraph D6.77*). |

Source: ANAO, based on PSM (Part D).

3.20 Based on the calculated processing error rates,[42] the ANAO considers that the vast majority of security clearances granted by the selected organisations between January 2005 and November 2007 met the audit criteria described in Table 3.2. That is, the information contained on the individual's personal security file was sufficient to fully justify the decision to grant the security clearance.

3.21 Specifically, 95 per cent or more of the security clearances granted by three of the selected organisations during the period being examined met each of the five audit criteria. In the remaining organisation (Organisation B in Table 3.3), 95 per cent or more of the security clearances granted in that period met only two of the five audit criteria.

[42] The processing error rates determined from the examination of the sample of security clearances are unbiased population estimates. That is, they are accurate estimates of the error rates that would be obtained from an examination of the entire population, in each of the selected organisations, of security clearances granted in the period being tested.

## Table 3.3

### Extent to which security clearances granted in the period January 2005 to November 2007 met the audit criteria

| | Organisation | | | |
|---|---|---|---|---|
| Criteria | A | B | C | D |
| Security clearance request | ✓ | ✖ | ✓ | ✓ |
| Information forms and consents | ✓ | ✓ | ✓ | ✓ |
| Mandatory personal documentation | ✓ | ✖ | ✓ | ✓ |
| Checks and inquiries | ✓ | ✖ | ✓ | ✓ |
| Clearance decision | ✓ | ✓ | ✓ | ✓ |

Note: ✓ - more than 95 per cent of the security clearances satisfied the audit criterion.
✖ - less than 95 per cent of the security clearances satisfied the audit criterion.

Source: ANAO, based on results of testing.

3.22 The main shortcomings identified during the examination of security clearances were:

- around 5 per cent of requests for security clearance forms in one organisation did not always clearly identify the reason the security clearance was required, nor indicate whether the duties of the position required access to security classified information or resources; and
- at another organisation:
  - o none of the personal security files contained a formal request for security clearance;
  - o around 12 per cent of the personal security files did not contain a copy of the individual's full birth certificate;
  - o around 24 per cent of the copies of birth certificates and 15 per cent of the copies of marriage certificates were not properly certified; and
  - o there was a general lack of evidence to indicate that the individual's background had been assessed.

3.23 Background checking is an analytical component of a security clearance assessment. Amongst other things, it involves substantiating information supplied by the individual, including verifying or corroborating its accuracy and assessing that information for any gaps or inconsistencies. During the audit, most of the personal security files examined at three organisations contained evidence of such analysis, including the use of checklists, hand-written notes on the information supplied by the individual and, in some cases, separately prepared reports detailing results of the assessment.

3.24 Conversely, one organisation advised the ANAO of its policy to only include evidence of specific matters on personal security files if they are noted during the conduct of checks, including any information that may cast doubt on the character or suitability of the clearance subject. The ANAO considers that this approach does not provide a full record that sufficient background checking has been undertaken.

## Suitability indicators

3.25 Assessing an individual's suitability to protect security classified information or resources is central to the security clearance process. The PSM (Part D) states that the assessment of suitability:

> involves carefully weighing of a number of variables relating to a clearance subject's background and character to make an accurate assessment.[43]

3.26 The PSM also identifies (and describes) the following characteristics as relevant to the assessment of an individual's suitability: honesty; trustworthiness; maturity; tolerance; loyalty; and attitude. In addition, it highlights potential areas of risk or vulnerability that may detract from, or cast doubt on, the suitability of the individual. These include issues arising from: the individual's financial status; their level of alcohol or drug use; any adverse personality traits; or occasions involving unfavourable conduct or behaviour.[44]

### Findings of the previous audit

3.27 Although all the organisations involved in Audit Report No.22 2001–02 demonstrated an awareness and understanding of the suitability factors contained in the PSM, most were unable to demonstrate they explicitly applied these factors during the clearance process. Three organisations used tools (such as checklists or questionnaires) to focus assessments of suitability towards issues relevant to the organisations' environment.

[43] PSM, op. cit., p. D19.

[44] ibid., p. D20.

Audit Report No.22 2001–02, Recommendation No. 6

The ANAO recommends organisations develop suitability indicators for use in security clearance assessments that are informed by organisation-specific risk/threat factors.[45]

## Findings of the current audit

Testing of security clearances identified an appropriate level of evidence of the consideration of organisation-specific suitability factors in two organisations, a lack of clear documented evidence in another organisation, while the remaining organisation planned to consider such factors as part of broader risk management reforms.

*Two* organisations had *fully* implemented this recommendation, *one* had *partially* implemented it and the *other* had *not* implemented it.

3.28 Three organisations had policy and guidance material on the conduct of suitability assessments. In each case, as well as describing the purpose of conducting suitability assessments and outlining the general suitability factors contained in the PSM, the material contained information on relevant organisation-specific suitability factors.

3.29 Table 3.4 describes some of the suitability factors and vulnerabilities (both generic and specific) that were contained in the policy and procedural material at the selected organisations.

[45] ANAO Audit Report No.22 2001–02, op. cit., p. 47.

## Table 3.4

### Suitability factors identified in policy and procedural material at the selected organisations

| Factor | Description |
|---|---|
| **Generic** | |
| Honesty | Demonstrated sincerity and truthfulness. Being helpful and frank. |
| Maturity | Ability for honest self-appraisal and an ability to cope with difficult situations, including dealing with constructive criticism. |
| Alcohol or drug abuse | May result in physical or behavioural issues, impact on reliability and the ability to make sound judgements. May also create financial difficulties. |
| Individual qualities | Does the clearance subject display: a disregard for rules or procedure; an over-dependence on others; superficial attention to detail; low levels of self-confidence; impulsiveness; indifference or lack of awareness or a pattern of repeated behaviour. |
| Tolerance | Understanding, accepting and respecting conflicting or alternative views or perspectives. |
| Personality traits | Personality characteristics or traits that indicate that the clearance subject may be susceptible to: a lack of stability; being unreliable; exercising poor judgment; being exploited or subject to undue influence. |
| Financial probity | Having a reasonable or sensible approach to the management of one's finances, including not being financially overextended. |
| **Specific** | |
| Born outside of Australia | Clearance subjects born outside of Australia and who meet certain criteria are interviewed. |
| Contacts and associates | Unreported or unexplained contacts or acquaintances with foreign officials and diplomats, political extremists, and criminal figures. |
| Security attitudes, including use of ICT | Previous experience demonstrates an understanding and acceptance of security principles and controls. A history of compliance with rules and requirements. |

Source: ANAO, based on the selected organisations.

3.30 The assessment of an individual's suitability to hold a security clearance is a critical part of the security clearance process. Judgements made against relevant and appropriate suitability indicators can help ensure that security clearance decisions are properly informed about security-related risks, threats or exposures. In this regard, the ANAO's testing of security clearances found an appropriate level of evidence of the consideration or assessment of suitability in two of the selected organisations.

**3.31** One of these organisations advised that it had recently introduced a form for use in the conduct of security clearances which required officers to explicitly make an assessment against a range of suitability factors and, as necessary, develop a risk management regime to deal with any concerns. The ANAO considers the adoption of this requirement to be a sound initiative as it supports a balanced assessment of the individual's suitability.

**3.32** However, in one organisation, there was generally insufficient evidence available to indicate that the suitability of individuals had been evaluated during the security clearance process. This organisation did not have any tools, such as a checklist, to record information about suitability assessments.

## Portability of security clearances

**3.33** To reduce unnecessary duplication in security clearance activity, security clearances should be readily portable or transferable between Australian Government organisations.

**3.34** The ANAO found broad support for the principle of the portability of Australian Government security clearances amongst the organisations involved in Audit Report No.22 2001–02. While acknowledging this support among these organisations, the JCPAA commented, in Report No.390, that it would be desirable to have a central co-ordinating organisation responsible for the maintenance of Australian Government security clearances, including administering the transfer of security clearances when staff moved between organisations.[46]

**JCPAA Report 390, Recommendation No. 9**

The Committee recommends the Attorney-General's Department report to the Committee on the cost effectiveness of maintaining a central database of security clearances.[47]

### Findings of the current audit

The Attorney-General's Department adequately advised the JCPAA about the cost effectiveness of maintaining a central database of security clearances, and implemented this recommendation.

[46] JCPAA Report 390, p. 61.

[47] ibid., p. 61.

3.35 In November 2003, the Attorney-General's Department (AGD) formally responded to the above recommendation, concluding:

> there are fundamental reasons why such an approach [maintaining a central database of security clearances] would not be effective.

3.36 In AGD's opinion, the more significant issue was the need to encourage greater portability of security clearances, while at the same time advocating that security clearance processes should be tailored to address organisation-specific security threats. To this end, AGD advised the JCPAA that the issue of portability would be addressed as part of a comprehensive review of existing personnel security policy. This review culminated in the release of the upgraded PSM in August 2005.

3.37 The ANAO's considers the enhancements to the PSM released in 2005 provided a sound framework for improving the portability of security clearances amongst Australian Government organisations. For example, paragraph D2.4 states:

> security clearances should be readily portable between agencies to reduce duplication of processes, and to enable the more efficient use of resources.

3.38 The ANAO notes that the results of the annual Australian Government Protective Security survey suggest an improvement in the management of portability amongst those Australian Government organisations that operate under the FMA Act since the release of the amended PSM in 2005.[48]

3.39 During 2004, AGD commenced work on a business case for the establishment of a centralised system for managing security clearances of contractors working in Australian Government organisations. AGD advised the ANAO that the Protective Security Policy Committee subsequently concluded that such a system would not be effective. Amongst the reasons put forward to support this view were that:

- a centralised system may lack flexibility, for example, to deal with cases requiring a particular priority in order to meet organisation-specific requirements; and

[48] The 2006 Australian Government Protective Security survey reported that 87 per cent of FMA Act agencies had procedures dealing with the recognition and acceptance of security clearance granted by other Australian Government organisations. This is an improvement on the result contained in the 2004 survey, which reported that 79 per cent of FMA Act agencies had procedures relating to the recognition of security clearances.

- there may be a potential lack of capacity for the employing organisation, if they desired, to undertake additional checks above minimum standards.

3.40 However, despite the apparent improvements noted in the annual Australian Government Protective Security survey, the ANAO notes that concerns remain about the portability of security clearances, particularly clearances for contracted service providers. Given this concern, and also due to advancements in technology, the ANAO considers it is appropriate to revisit the issue of establishing a centralised clearance system.

3.41 In this regard, the ANAO acknowledges that AGD is currently examining the feasibility of a central record of clearances for ICT professionals.[49] The results of this work should enable AGD to identify and assess opportunities of using a centralised system to record and administer Australian Government security clearances more broadly.

3.42 AGD advised the ANAO that it is also conducting a review of security clearance arrangements. The review will identify options to achieve efficiencies in security clearance processes and examine the feasibility of establishing a central vetting agency.

[49] This is in response to the report of the Professional and Skills Development Taskforce, *Meeting the Demand for ICT Skills in the Australian Public Service – Today and for the Future*, Australian Government Information Management Office, Canberra, August 2007, p. 6.

# 4. Maintaining Security Clearances

*This chapter addresses the implementation of those recommendations from the previous reports that were designed to improve processes for managing the ongoing appropriateness and currency of security clearances.*

## Introduction

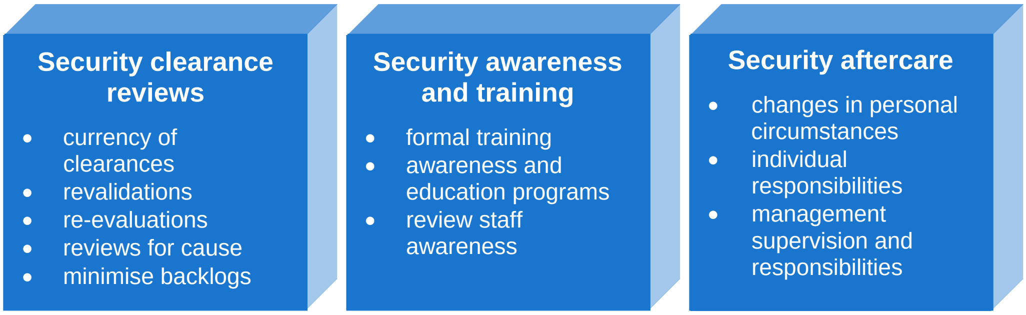
4.1 Subjecting security clearances to regular maintenance allows for an assessment of whether initial security clearances remain valid and provides an opportunity to identify emerging issues or risks. Effective maintenance of security clearances involves:

- promoting and reinforcing security awareness throughout the organisation, including providing a security education program;
- periodically reviewing each security clearance; and
- monitoring any changes in circumstances or issues impacting on the continued suitability of a clearance subject to hold a security clearance.

4.2 Figure 4.1 illustrates key issues involved in the maintenance of security clearances that are examined in this chapter.

### Figure 4.1

**Maintaining security clearances**



**Security clearance reviews**

- currency of clearances
- revalidations
- re-evaluations
- reviews for cause
- minimise backlogs

**Security awareness and training**

- formal training
- awareness and education programs
- review staff awareness

**Security aftercare**

- changes in personal circumstances
- individual responsibilities
- management supervision and responsibilities

Source: ANAO.

4.3 In this context, the ANAO examined the extent to which the selected organisations implemented the following recommendations:

- Audit Report No.22 2001–02, Recommendation No. 8, 9 and 10; and
- JCPAA Report 390, Recommendation No. 7.

## Security clearance reviews

4.4 Over time, changes in personal and an organisation's circumstances may give rise to new factors relevant to an individual's need for, or suitability to hold, a security clearance. In this context, organisations must have a formal program to assess the continuing appropriateness and currency of security clearances. The PSM (Part D) requires, at a minimum, that security clearance review processes comprise:

- revalidations—undertaken at certain intervals to update an individual's information, including confirming the ongoing need to access security classified information and identifying any changes in circumstances;
- re-evaluations—undertaken at certain intervals[50] to comprehensively re-assess the continued suitability of an individual to have a security clearance; and
- reviews for cause—undertaken whenever a security concern regarding a security clearance holder arises. The review might either be done as a revalidation, a re-evaluation or an investigation into the specific concern.

### Findings of the previous audit and JCPAA review

4.5 Four of the organisations involved in Audit Report No.22 2001–02 were not effectively managing security clearance review processes. In particular, the ANAO considered the organisations did not have the capacity to overcome backlogs in the conduct of clearance reviews.

Audit Report No.22 2001–02, Recommendation No. 8

It is recommended organisations consider taking concerted efforts to overcome the current backlog in the conduct of security clearance reviews as a matter of priority and ensure these processes are carried out in a timely manner in the future.[51]

4.6 In Report 390, the JCPAA stated that organisations generally had not made sufficient resources available to maintain new clearance requirements or to avoid, or deal with, the backlog of security clearance re-evaluations.[52]

[50] The minimum time frames for conducting revalidations and re-evaluations are illustrated on page D47 of the PSM.

[51] ANAO Audit Report No.22 2001–02, op. cit., p. 53.

[52] JCPAA Report 390, op. cit., p. 58.

JCPAA Report 390, Recommendation No. 7

The JCPAA recommends organisations allocate the resources necessary to bring their security clearance processes in line with the requirements of the Protective Security Manual.[53]

## Findings of the current audit

The selected organisations had no or minimal backlogs of security clearance reviews. This achievement arose from a mix of additional resourcing and improved processes.

*Two* organisations had *fully* implemented ANAO Recommendation No. 8, *one* had *substantially* implemented it, while the *other* organisation had *partially* implemented it.

*Three* organisations had *fully* implemented JCPAA Recommendation No. 7 and *one* had *partially* implemented it.

4.7 The previous ANAO audit estimated that the proportion of out-of-date security clearance reviews in the selected organisations ranged from 'zero to around 10 per cent of total security clearances (in the best cases) and up to around 45 per cent (in the worst cases)'.[54]

4.8 The current audit found a substantial improvement in the level of out-of-date security clearance reviews. One of the selected organisations was also examined in the previous audit (Organisation A and 1 in Figure 4.2).[55] In this organisation, the proportion of SECRET and TOP SECRET security clearance reviews that were overdue fell from 45 per cent in the previous audit to 6 per cent in the current audit. Moreover, the proportion of security clearance reviews that were overdue in other selected organisations were 3 per cent in one organisation and zero in the other two. Overall, Figure 4.2 shows that the level of out-of-date security clearance reviews for the four selected organisation was substantially lower than for the organisations involved in the previous audit.

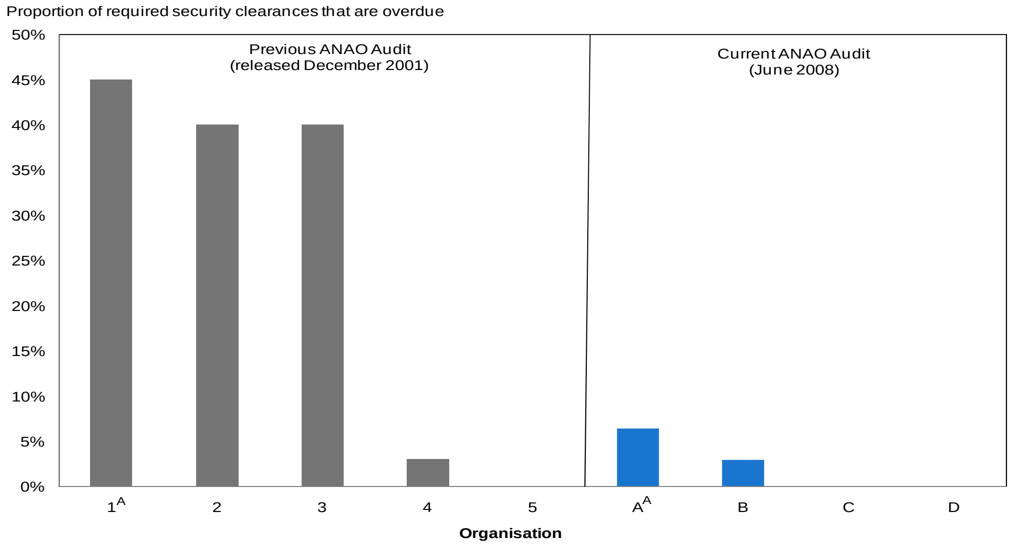
[53] ibid., p. 59.

[54] ANAO Audit Report No.22 2001–02, op. cit., p. 51.

[55] ibid.

## Figure 4.2

### Backlog of security clearance reviews, previous and current previous audits



Notes: (A) Organisation 1 and A are the same. The proportion of overdue security clearance cited for this organisation relates to SECRET and TOP SECRET clearances only.

Source: ANAO testing and ANAO Audit Report No.22 2001–02.

### *Increase in resources allocated to security clearance processes*

4.9 Since the previous audit, three of the selected organisations had increased the level of resources allocated to the conduct and administration of security clearances. Actions taken by these organisations included:

- recruiting additional security clearance staff;
- engaging non-ongoing (short term) contractors to assist meet workload peaks; and
- in one case, establishing a panel of contracted security clearance providers.

4.10 The remaining organisation outsourced its security clearance requirements and, at the time of the audit, did not require any additional resources to meet its security clearance workload (including reviews).

### *Processes for managing security clearance reviews*

4.11 The audit found a significant improvement in the processes used in the management of security clearance reviews. For example, each of the selected organisations had formal arrangements in place for identifying and actioning security clearance review requirements in a timely manner. Two better practices identified during the audit were:

- one organisation monitored security clearance review requirements six months in advance of their due date; and
- one organisation had improved administration and associated workflow by allocating responsibility for the identification and management of security clearance reviews to a dedicated team.

4.12 However, in the two organisations that had out-of-date security clearance reviews, the audit found that around 60 per cent of these reviews were overdue by more than 12 months. Paragraph D10.21 of the PSM (2005) states that security clearances that have not been re-evaluated within 12 months of their nominal expiry date are deemed to have lapsed. This means that the holders of these clearances are no longer entitled to access security classified information or resources.

4.13 In September 2007, the Chief Executive at one of the organisations approved the extension of a waiver (as provided for in paragraph A1.15 of the PSM) from the requirement relating to lapsing security clearances.[56] Approving this waiver was part of a multi-faceted strategy adopted by this organisation to manage overdue security clearance reviews. As demonstrated in Figure 4.2, the organisation (Organisation 1 and A) made considerable progress in reducing the number of overdue security clearance reviews since the previous ANAO audit.

4.14 At the time of the audit, the other organisation did not have a waiver in place. The existence of security clearances that have lapsed, and which have not been formally cancelled, potentially poses a significant security risk. Furthermore, assuming the clearance holder still requires the security clearance, restricting their access to security classified information is likely to detract from their ability to effectively fulfil their duties.

[56] The waiver has been approved for the period the organisation considers necessary to overcome the backlog, in this case, until 31 December 2010.

## Security awareness

4.15 The effectiveness of protective security systems depend, in part, on the level of awareness about and acceptance of the organisation's security principles and practices. To support the maintenance of a strong level of security awareness, organisations should have a formal program of security education and training.

4.16 Effective security education and training programs:

- increase staff interest in, and understanding of, protective security policies and practices;
- reduce resistance to security procedures;
- provide clarity on security-related roles and responsibilities;
- increase commitment to protecting the organisation's information and resources; and
- emphasise the risks of poor security practice, including explaining the implications of a breach of security.

### Findings of the previous audit

4.17 Low levels of awareness and understanding about personnel security responsibilities were identified amongst staff in three of the organisations involved in Audit Report No.22 2001–02. None of these organisations had implemented formal security education programs.

Audit Report No.22 2001–02, Recommendation No. 9

The ANAO recommends organisations review the effectiveness of personnel security awareness and education programs to improve the identification, monitoring and promotion of personnel security issues.[57]

### Findings of the current audit

Three organisations had effective personnel security awareness and education programs. The other organisation did not provide training on a systematic basis.

*Three* organisations had *fully* implemented this recommendation and *one* had *partially* implemented it.

[57] ANAO Audit Report No.22 2001–02, op. cit., p. 53.

4.18 The provision of sufficient security awareness material was recognised as important in the personnel security policy documentation at each of the selected organisations. To satisfy these policy requirements, each organisation had recently assessed their security awareness programs. However, these assessments encompassed a formal evaluation of the effectiveness of the strategies at only one selected organisation.

4.19 As a result of these assessments, the audit identified a number of examples of improvements to security awareness arrangements. These included the organisations:

- targeting security awareness training at supervisors;
- identifying the need to re-develop security education and training material (as well as a means to evaluate whether that material was effective in improving security awareness levels);
- engaging an external service provider to deliver security awareness training;
- re-designing the form and content of a security newsletter to improve its readability; and
- developing a formal communications strategy to guide decision-making on security awareness products.

4.20 One organisation advised that it had commenced an examination to re-assess whether its security awareness strategies were effectively meeting the organisation's needs, including identifying opportunities for more-targeted training.

4.21 Table 4.1 summarises the number of selected organisations that adopted particular security awareness strategies. Each of the selected organisations provided information in security clearance packs on the individual's ongoing responsibilities. This strategy represents a useful first step. However, maintaining an effective level of security awareness and understanding requires continuing reinforcement through a series of other approaches, such as regular security training or regularly publishing security newsletters.

## Table 4.1

### Security awareness strategies used by the selected organisations

| Security awareness strategy | Number of the four organisations that used this strategy |
|---|---|
| Security clearance packs include information on the individual's ongoing responsibilities. | 4 |
| Providing access to on-line security-learning applications. | 3 |
| Displaying posters around the workplace to highlight key security-related messages. | 3 |
| Periodically distributing e-mail alerts or computer messages covering contemporary security issues. | 3 |
| Formal security awareness training or information sessions provided to staff. | 2 |
| Individually tailored or targeted security awareness briefings or training on request or to address areas of concern or risk. | 2 |
| Providing staff with kits, pamphlets or checklists containing tips on good security practices. | 2 |
| Issuing security newsletters or bulletins to provide advice on protective security issues and guidance on compliance with security requirements. | 2 |

Source: ANAO.

4.22 At the time of the audit, three organisations were providing formal and structured security awareness training to their staff, either face-to-face or through an on-line application. Each of these organisations was actively monitoring attendance at security training. In an example of a better practice, one of the organisations required attendance at security training to be included as a standard capability in all individual performance agreements.

4.23 The remaining organisation did not provide security education or awareness training on a structured or regular basis. Rather, it was delivered irregularly as resources allowed. Furthermore, no records were kept of attendance at this training.

## Security aftercare

4.24 The term 'security aftercare' describes the practices used in the timely identification, and assessment, of issues relevant to an individual's ongoing suitability to hold a security clearance. These practices complement, but are not a substitute for the clearance review and security education processes.

### Findings of the previous audit

4.25 Most of the organisations involved in Audit Report No.22 2001–02 did not have effective processes for identifying and monitoring emerging issues relevant to the ongoing suitability of individuals.

Audit Report No.22 2001–02, Recommendation No. 10

The ANAO recommends organisations review and improve the effectiveness of processes for the early identification of issues related to an individual's continued suitability to hold a security clearance.[58]

### Findings of the current audit

Two organisations had effective security aftercare arrangements and two organisations did not.

*Two* organisations had *fully* implemented this recommendation while the other two organisations had *not* implemented it.

4.26 Two organisations had a range of processes for managing security aftercare issues. These processes included: implementing tailored and dedicated aftercare programs; providing clear guidelines or instructions; and regularly reinforcing the requirement for staff to report changes in circumstances and contracts.

4.27 In addition, both organisations regularly conducted security inspections. During the examination of security clearances, the ANAO observed a number of instances where issues identified during these inspections were recorded on individual's personal security file. In these cases, the personal security file indicated that the impacts, if any, on the person's security clearance had been assessed.

[58] ibid., p. 54.

**4.28** Conversely, the two other organisations did not have clear security aftercare arrangements. In particular, they lacked formal processes, outside of clearance reviews, to systematically identify issues relevant to the ongoing suitability of individuals.

**4.29** Systematic and well-structured security aftercare processes, including measures to monitor the continued suitability of individuals, are important to assist organisations maintain the appropriateness and currency of personal security clearances.

## Recommendation No.2

**4.30** The ANAO recommends that organisations clearly specify security aftercare arrangements and promote these arrangements in security education and training activities.

### Organisations' responses to the recommendation

**4.31** Each of the audited organisations agreed with the recommendation.

Steve Chapman
Acting Auditor-General

Canberra ACT
18 June 2008

# Appendices

# Appendix 1: Main Changes in Personnel Security Policy in the PSM

Table A1 illustrates significant changes in personnel security policy between the 2000 and 2005 versions of Part D of the PSM.

## Table A1

### Summary of main changes in Part D of the PSM (2005)

| |
|---|
| Inclusion of the statement that 'security clearances should be readily portable between agencies to reduce duplication of processes, and to enable the more efficient use of resources'—D2.4. |
| New Chapter 6 titled 'Standards for conducting security clearances' containing, amongst other things, additional guidance on the conduct of background assessments, and new guidance on uncheckable backgrounds and personal vulnerabilities. |
| Introduction of the 'Medical Supplement' - a form that can be used to assist collect information about a clearance subject's health and medical conditions—D7.34. |
| Clarification on the types of personal documentation that are mandatory (if applicable) and the personal documentation that 'may assist identity verification' or 'may be used as an alternative source of corroborating evidence'—D7.42/44. |
| Clarification on the level of security clearances that require contact with referees and the minimum number of referees required—D7.92/94. |
| Inclusion of the statement that organisations 'should consider using a range of supplementary procedures to complement the minimum standards'—D7.111. |
| Provision of more information on challenging security clearance decisions, including the rights of clearance subjects and establishing internal review processes—D9. |
| Extending the interval for conducting re-evaluations of SECRET and HIGHLY PROTECTED security clearances from a period 'not exceeding five years' to 'every nine years' if revalidations are conducted 'every three years'—D10.23. |
| Inclusion of the statement that organisations should conduct 'a review for cause whenever a security concern regarding a security clearance holder arises'—D10.25. |

Source: ANAO, based on the PSM (2005).

# Appendix 2: Summary of Progress Against Recommendations in the Previous ANAO Audit Reports and JCPAA Report

| Recommendation | Progress |
|---|---|
| ***ANAO Audit Report No.22 2001–02*** | |
| **Recommendation No. 1:** The ANAO recommends that organisations approve and promulgate appropriate policy and procedures to support the conduct and administration of personnel security. | Fully implemented - one organisation<br>Substantially implemented - two organisations<br>Partially implemented - one organisation |
| **Recommendation No. 2:** The ANAO recommends that organisations review their security risk management processes to ensure, in particular, that personnel security threats and hazards are thoroughly considered and that organisation-specific security risks are appropriately factored into the security clearance process. | Fully implemented - one organisation<br>Partially implemented - two organisations<br>Not implemented - one organisation |
| **Recommendation No. 3:** The ANAO recommends that organisations periodically review registers of Designated Security Assessment Positions and Positions of Trust to ensure they accurately reflect security clearance requirements and organisations develop appropriate guidelines to assist managers to undertake position assessments. | Fully implemented - one organisation<br>Substantially implemented - two organisations<br>Partially implemented - one organisation |
| **Recommendation No. 4:** The ANAO recommends that organisations adopt better practice contract management principles and standards in outsourced security clearance and vetting service arrangements. | Substantially implemented - three organisations<br>N/A - one organisation |
| **Recommendation No. 5:** The ANAO recommends that organisations record all information collected during the course of a security clearance on the subject's personal security file. | Fully implemented - three organisations<br>Partially implemented - one organisation |

| Recommendation | Progress |
|---|---|
| **Recommendation No. 6:** The ANAO recommends that organisations develop suitability indicators for use in security clearance assessments which are informed by organisation-specific risk/ threat factors. | Fully implemented - two organisations<br>Partially implemented - one organisation<br>Not implemented - one organisation |
| **Recommendation No. 7:** The ANAO recommends that organisations assess opportunities to integrate personnel security information into the organisation's Human Resource Management Information System or other appropriate corporate system. | Fully implemented - two organisations<br>Substantially implemented - one organisation<br>Partially implemented - one organisation |
| **Recommendation No. 8:** The ANAO recommends that organisations consider taking concerted efforts to overcome the current backlog in the conduct of security clearance reviews as a matter of priority and ensure these processes are carried out in a timely manner in the future. | Fully implemented - two organisations<br>Substantially implemented - one organisation<br>Partially implemented - one organisation |
| **Recommendation No. 9:** The ANAO recommends that organisations review the effectiveness of security awareness and education programs to improve the identification, monitoring and promotion of personnel security issues. | Fully implemented - three organisations<br>Partially implemented - one organisation |
| **Recommendation No. 10:** The ANAO recommends that organisations review and improve the effectiveness of processes for the early identification of issues related to an individual's continued suitability to hold a security clearance. | Fully implemented - two organisations<br>Not implemented - two organisations |

| Recommendation | Progress |
|---|---|
| ***ANAO Audit Report No.15 2003–04*** | |
| **Recommendation No. 1:** The ANAO recommends that Finance strengthen monitoring procedures to ensure MOP(S) Act staff for whom a security clearance is outstanding are identified in a timely manner, and that appropriate follow-up is undertaken with relevant staff members, their employing Parliamentarians and the security-vetting agency undertaking the security clearance. | Implemented – Finance |
| ***JCPAA Report No. 390*** | |
| **Recommendation No. 7:** The Committee recommends all agencies allocate the resources necessary to bring their security clearance processes in line with the requirements of the Protective Security Manual. | Fully implemented – three organisations<br>Partially implemented – one organisation |
| **Recommendation No. 8:** The Committee recommends all agencies make the necessary changes to their Human Resource Management Information System to support management reporting in relation to security clearances and appropriate access to security clearance information. | Fully implemented - two organisations<br>Not implemented - one organisation<br>Not applicable – one organisation |
| **Recommendation No. 9:** The Committee recommends the Attorney-General's Department report to the Committee on the cost effectiveness of the Department maintaining a central database of security clearances. | Implemented – AGD |

Source: ANAO.

# Appendix 3: Protective Security Audits Undertaken by the ANAO

Since 1995, the ANAO has completed the following cross-agency protective security audits:

- Audit Report No.21 1996–97, *Protective Security;*
- Audit Report No.7 1999–00, *Operation of the Classification System for Protecting Sensitive Information;*
- Audit Report No.22 2001–02, *Personnel Security—Management of Security Clearances;*
- Audit Report No.23 2002–03, *Physical Security Arrangements in Commonwealth Agencies;*
- Audit Report No.55 2003–04, *Management of Protective Security;*
- Audit Report No.41 2004–05, *Administration of Security Incidents, including the Conduct of Security Investigations;*
- Audit Report No.23 2005–06, *IT Security Management;* and
- Audit Report No.43 2006–07, *Managing Security Issues in Procurement and Contracting.*

# Appendix 4: Schedule of Sub-criteria Used in the Examination of Security Clearances

| Item | Audit Criterion |
|---|---|
| **1** | **Request for Security Clearance** |
| 1.1 | Clearance subject's full name |
| 1.2 | Clearance subject's work area and contact details |
| 1.3 | Reason the security clearance is required |
| 1.4 | Whether the job is, or has been, identified as a DSAP or PoT or the duties require access to security classified resources, and |
| 1.5 | Advice whether the clearance subject has been cleared previously and if so, where, when and to what level. |
| **2** | **Information documents and consent forms** |
| 2.1 | Information Letter |
| 2.2 | Schedule of Personal Documentation |
| 2.3 | General Consent Form |
| 2.4 | Official Secrecy Acknowledgment Form |
| 2.5 | Personal Particulars Form |
| 2.6 | Financial declarations and questionnaires |
| 2.7 | Authorisation for the Release of Medical Information (if required) |
| 2.8 | Statutory Declaration (if required) |
| **3** | **Personal documentation (all documentation should be certified copies)** |
| 3.1 | Full birth certificate |
| 3.2 | Change of name certificate (if applicable) |
| 3.3 | Naturalisation or citizenship certificate (if applicable) |
| 3.4 | Current marriage certificate (if applicable) |
| 3.5 | Decree nisi or decree absolute (if applicable) |
| 3.6 | Military discharge certificate (if applicable) |
| **4** | **Checks and inquiries** |
| 4.1 | Background Check |
| 4.2 | Bankruptcy check (if required) |
| 4.3 | Police check |
| 4.4 | ASIO security assessment (if required) |
| 4.5 | Workplace and personal referees (if required) |
| 4.6 | Clearance subject interviews (if required) |
| **5** | **Advice of the clearance decision** |
| 5.1 | Grant letter/notice |
| 5.2 | Recommendation by vetting official |
| 5.3 | Approval by delegate |

Source: ANAO, based on the PSM.

# Series Titles

Audit Report No.1 2007–08
*Acquisition of the ABRAMS Main Battle Tank*
Department of Defence
Defence Materiel Organisation

Audit Report No.2 2007–08
*Electronic Travel Authority Follow-up Audit*
Department of Immigration and Citizenship

Audit Report No.3 2007–08
*Australian Technical Colleges Programme*
Department of Education, Science and Training

Audit Report No.4 2007–08
*Container Examination Facilities Follow-up*
Australian Customs Service

Audit Report No.5 2007–08
*National Cervical Screening Program Follow-up*
Department of Health and Ageing

Audit Report No.6 2007–08
*Australia's Preparedness for a Human Influenza Pandemic*
Department of Health and Ageing
Department of Agriculture, Fisheries and Forestry

Audit Report No.7 2007–08
*The Senate Order for Departmental and Agency Contracts (Calendar Year 2006 Compliance)*

Audit Report No.8 2007–08
*Proof of Identity for Accessing Centrelink Payments*
Centrelink
Department of Human Services

Audit Report No.9 2007–08
*Australian Apprenticeships*
Department of Education, Science Training

Audit Report No.10 2007–08
*Whole of Government Indigenous Service Delivery Arrangements*

Audit Report No.11 2007–08
*Management of the FFG Capability Upgrade*
Department of Defence
Defence Materiel Organisation

Audit Report No.12 2007–08
*Administration of High Risk Income Tax Refunds in the Individuals and Micro Enterprises Market Segments*
Australian Taxation Office

Audit Report No.13 2007–08
*The Australian Taxation Office's Approach to Managing Self Managed Superannuation Fund Compliance Risks*
Australian Taxation Office

Audit Report No.14 2007–08
*Performance Audit of the Regional Partnerships Programme:*
*Volume 1–Summary and Recommendations*
*Volume 2–Main Report*
*Volume 3–Project Case Studies*
Department of Transport and Regional Services

Audit Report No.15 2007–08
*Administration of Australian Business Number Registrations: Follow-up Audit*
Australian Taxation Office

Audit Report No.16 2007–08
*Data Integrity in the Child Support Agency*
Child Support Agency
Department of Human Services

Audit Report No.17 2007–08
Management of the IT Refresh Programme
Centrelink

Audit Report No.18 2007-08
*Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2007*

Audit Report No.19 2007–08
*Administration of the Automotive Competitiveness and Investment Scheme*
Department of Innovation, Industry, Science and Research
Australian Customs Service

Audit Report No.20 2007–08
*Accuracy of Medicare Claims Processing*
Medicare Australia

Audit Report No.21 2007–08
*Regional Delivery Model for the Natural Heritage Trust and the National Action Plan for Salinity and Water Quality*
Department of the Environment, Water, Heritage and the Arts
Department of Agriculture, Fisheries and Forestry

Audit Report No.22 2007–08
*Administration of Grants to the Australian Rail Track Corporation*
Department of Infrastructure, Transport, Regional Development and Local Government

Audit Report No.23 2007–08
*The Management of Cost Recovery by Selected Regulators*

Audit Report No.24 2007–08
*DIAC's Management of the Introduction of Biometric Technologies*
Department of Immigration and Citizenship

Audit Report No.25 2007–08
*Administering Round the Clock Medicare Grants*
Department of Health and Ageing

Audit Report No.26 2007–08
*Tasmanian Forest Industry Development and Assistance Programs*
Department of Agriculture Fisheries and Forestry

Audit Report No.27 2007–08
*Emergency Management Australia*
Attorney-General's Department

Audit Report No.28 2007–08
*Defence's Compliance with the Public Works Committee Approval Processes*
Department of Defence

Audit Report No.29 2007–08
*Parent School Partnerships Initiative*
Department of Education, Employment and Workplace Relations

Audit Report No.30 2007–08
*The Australian Taxation Office's Use of Data Matching and Analytics in Tax Administration*
Australian Taxation Office

Audit Report No.31 2007–08
*Management of Recruitment in the Australian Public Service*

Audit Report No.32 2007–08
*Preparation of the Tax Expenditures Statement*
Department of the Treasury

Audit Report No.33 2007–08
*The National Capital Authority's Management of National Assets*
National Capital Authority

Audit Report No.34 2007–08
*Administration of the Pathology Quality and Outlays Memorandum of Understanding*
Department of Health and Ageing

Audit Report No.35 2007–08
*Building Certification of Residential Aged Care Homes*
Department of Health and Ageing

Audit Report No.36 2007–08
*The Australian Taxation Office's Strategies to Address Tax Haven Compliance Risks*
Australian Taxation Office

Audit Report No.37 2007–08
*Management of Credit Cards*

Audit Report No.38 2007–08
*Administration of Job Network Service Fees*
Department of Education, Employment and Workplace Relations

Audit Report No.39 2007–08
*Managing e-Business Applications—Follow-up Audit*
Department of Education, Employment and Workplace Relations

Audit Report No.40 2007–08
*Taxpayers' Charter—Follow-up Audit*
Australian Taxation Office

# Current Better Practice Guides

*The following Better Practice Guides are available on the Australian National Audit Office Website.*

| | |
|---|---|
| Agency Management of Parliamentary Workflow | May 2008 |
| Public Sector Internal Audit | |
| An Investment in Assurance and Business Improvement | Sep 2007 |
| Fairness and Transparency in Purchasing Decisions | |
| Probity in Australian Government Procurement | Aug 2007 |
| Administering Regulation | Mar 2007 |
| Developing and Managing Contracts | |
| Getting the Right Outcome, Paying the Right Price | Feb 2007 |
| Implementation of Programme and Policy Initiatives: | |
| Making implementation matter | Oct 2006 |
| Legal Services Arrangements in Australian Government Agencies | Aug 2006 |
| Preparation of Financial Statements by Public Sector Entities | Apr 2006 |
| Administration of Fringe Benefits Tax | Feb 2006 |
| User–Friendly Forms | |
| Key Principles and Practices to Effectively Design and Communicate Australian Government Forms | Jan 2006 |
| Public Sector Audit Committees | Feb 2005 |
| Fraud Control in Australian Government Agencies | Aug 2004 |
| Security and Control Update for SAP R/3 | June 2004 |
| Better Practice in Annual Performance Reporting | Apr 2004 |
| Management of Scientific Research and Development Projects in Commonwealth Agencies | Dec 2003 |
| Public Sector Governance | July 2003 |
| Goods and Services Tax (GST) Administration | May 2003 |
| Building Capability—A framework for managing learning and development in the APS | Apr 2003 |
| Internal Budgeting | Feb 2003 |
| Administration of Grants | May 2002 |
| Performance Information in Portfolio Budget Statements | May 2002 |

| | |
|---|---|
| Some Better Practice Principles for Developing Policy Advice | Nov 2001 |
| Rehabilitation: Managing Return to Work | June 2001 |
| Business Continuity Management | Jan 2000 |
| Building a Better Financial Management Framework | Nov 1999 |
| Building Better Financial Management Support | Nov 1999 |
| Commonwealth Agency Energy Management | June 1999 |
| Security and Control for SAP R/3 | Oct 1998 |
| Controlling Performance and Outcomes | Dec 1997 |
| Protective Security Principles (in Audit Report No.21 1997–98) | Dec 1997 |