The Auditor-General
Audit Report No.22 2001–2002
Protective Security Audit

Personnel Security—
Management of Security Clearances

Australian National Audit Office

ISSN 1036-7632

ISBN 0 642 80603 9

Australian National
Audit Office

Canberra ACT
4 December 2001

Dear Madam President
Dear Mr Speaker

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

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

P. J. Barrett
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.

Auditor-General reports are available from Government Info Shops. Recent titles are shown at the back of this report.

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

Richard Rundle
Bill Bonney
Andrew Rowe
Rebecca Lindwall
Fleur Spriggs

Contents

Abbreviations/Glossary

ANAO	Australian National Audit Office
ASA	Agency Security Adviser
ASIO	Australian Security Intelligence Organisation
ASVS	Australian Security Vetting Service
DSAP	Designated Security Assessment Position
HRMIS	Human Resource Management Information System
IT	Information Technology
NSC	National Security Committee of Cabinet
NV	Negative vet
POT	Position of Trust
PSB	Protective Security Bulletin
PSCC	Protective Security Coordination Centre
PSF	Personal Security File
PSM	Protective Security Manual
PSPC	Protective Security Policy Committee
PV	Positive vet

Summary and Recommendations

Summary

Background

1. Protective security concerns the protection of information, assets and human resources from potential threats. It includes physical security (eg, building access control), personnel security (eg, background investigations), information security (eg, classification of documents), and computer and communications security (eg, IT access controls).

2. This audit was undertaken as part of the Australian National Audit Office's (ANAO) protective security audit program and was prompted by the findings of the previous ANAO protective security audit referred to below. It is considered timely given events over the past two years that have increased the profile of protective security (including personnel security) in the Commonwealth. This includes the release of the new Protective Security Manual (PSM) in December 2000 and several high profile security breaches.

3. In 1996, the ANAO undertook an audit of the security classification of information in Commonwealth organisations.[1] The main objectives of the audit were to determine whether organisations were protecting sensitive information in accordance with the PSM and better practice standards. Among other things, the audit concluded there was...

> *...a high risk of unauthorised access to sensitive information, particularly in relation to staff and other people dealing with the organisations, such as contractors and clients.*

4. Specifically, in relation to security clearances, the 1996 audit found:

- a high proportion of staff had clearances in excess of work requirements;
- some staff had access to information for which they were not cleared, particularly during the long lead time for obtaining initial clearances; and
- most organisations did not maintain the currency of their security clearances.

---

1 ANAO Audit Report No.7, 1999–2000, *Operation of the Classification System for Protecting Sensitive Information*.

Audit objectives and focus

5. The objective of this audit was to determine if organisations were managing security clearance and vetting processes effectively and efficiently and in accordance with Commonwealth policy, as outlined in PSM 2000. It was also intended the audit would provide recommendations for improvement (where necessary) and identify and disseminate any identified better practice.

6. In the interests of establishing better practice, organisations were assessed against the requirements of PSM 2000.[2]

7. In relation to personnel security the main changes included in PSM 2000 relate to the:

- requirement that clearance subjects be Australian citizens;
- extension of checkable background periods for Protected and Highly Protected level clearances;
- requirement that checks be made with previous employers for the most recent significant employment details; and
- tightening of requirements for re-validations (previously known as re-examination) and re-evaluations (previously known as review) of security clearances.

8. The audit focussed on those security clearances which comprise the process known as 'negative 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. It can be distinguished from 'positive vetting', which attempts to establish beyond reasonable doubt the suitability of the clearance subject to hold the requested security clearance.[3]

9. The audit evaluated the security clearance and vetting policies and practices of seven organisations against four key audit criteria. Within each audit criteria, more detailed evaluation criteria were developed using material gathered from research into Commonwealth Public Sector and international sources. Some of the evaluation criteria were not applicable to one of the organisations and the latter was therefore not assessed against these. Tables 2.1 to 2.12 in the '*Audit Findings*' section of this report indicate the number of organisations reviewed against the nominated evaluation criteria.

---

2 Refer to Appendix 1 for further background on the decision to utilise PSM 2000 for this audit and to Appendix 2 for an overview of PSM 2000.

3 Attorney-General's Department, *Commonwealth Protective Security Manual 2000*, Commonwealth of Australia, Glossary.

10. The key audit criteria the organisations were evaluated against, where applicable, and their components, were:

- General Management: position assessments, policies and procedures, risk management, quality control processes, and the qualifications and capabilities of Agency Security Advisers (ASA) and other vetting staff;
- Pre-screening and Employment Checking: clearance portability, clearance eligibility standards, pre-clearance access controls, and contractor clearances;
- Assessment and Decision processes: documentation and record-keeping, minimum standards, decision and appeal processes; and
- Maintenance, Monitoring and Review: clearance maintenance and review, information management, security awareness and education programs.

11. The audit criteria are explained in more detail in Appendix 1.

Audit conclusion

12. Part D of PSM 2000 provides an effective framework for the management of personnel security. While security clearance policy and procedures of organisations were consistent with the requirements of the PSM, overall the audit found shortcomings in relation to the management, resourcing and operation of personnel security. Among the organisations examined the audit encountered a backlog of initial clearances, poor clearance aftercare processes, inadequate security information management and a failure to establish and enforce appropriate procedures to re-validate initial clearances in an acceptable timeframe. As a result, these organisations were exposed to breakdowns in the operation of their personnel security process which, amongst other things, may lead to inappropriate access to classified information. This problem is compounded when these issues occur in organisations which have not prepared, or which have inadequate risk management plans to appropriately integrate protective security risk management priorities into the organisation's overall risk management requirements.

13. In light of this situation, the ANAO suggests that all organisations with a personnel security requirement review their personnel security arrangements as a matter of priority. This review should include, but not necessarily be limited to:

- carrying out a risk management review of protective security arrangements and integrating the results of the review into organisation-wide risk planning;

- developing and implementing a process for clearing any backlog of initial clearances;
- actively seeking ways to reduce the processing cycle time for security clearances, in conjunction with vetting service providers and contributors;
- implementing appropriate information support systems to effectively support the management of personnel security; and
- establishing processes for clearing any backlog of security clearance reviews and ensuring timely reviews in the future.

Audit findings

14. The audit found considerable scope for improvement in several important areas. The audit identified that the emphasis in personnel security in the organisations audited was on the initial security clearance process, often with little after-care and clearance maintenance focus or activity. Ongoing monitoring and the conduct of security clearance reviews[4] are essential to effective personnel security as most individuals who intentionally commit security violations or breaches against an employer do not begin their career or position with the intention to do so. Although some individuals may have a higher propensity to commit these acts, other crucial factors include availability or opportunity and the lack of effective control structures.[5] The most critical finding in this regard was that all but one organisation had a large number of security clearances overdue for review. A failure to maintain the currency of security clearances contravenes Part D, section 8 of PSM 2000.

15. The audit also found shortcomings in relation to the application of risk management principles to personnel security. Most organisations did not have an up-to-date protective security risk assessment as required by Part B of the PSM, and at the time of the audit, none had effectively integrated risk assessments into personnel security arrangements.

---

4 The PSM uses the terms 're-evaluation' and 're-validation' rather than 'review'; however for reasons of brevity and conciseness, the term 'review' is used throughout this report to refer to both 're-evaluations' and 're-validations.'

5 Refer to AIC Trends & Issues No.199, March 2001, *The Psychology of Fraud*, Australian Institute of Criminology.

16. In addition, effective information management systems were not in place to support personnel security in some organisations. Most organisations require improvements to ensure sufficient and timely management information is available to effectively support personnel security management, particularly the maintenance of security clearances and security assessed positions. This was also a key finding in the previous protective security audit on classification of information.

17. Apart from the above issues, the following instances of non-compliance with the requirements of Part D of PSM 2000 were also noted during the audit:

- maintenance, administration and disposal of personal security records (Part D, section 10); and
- maintenance of clearance documentation, including interview reports (Part D, section 6).

18. Finally, it was apparent in most organisations that insufficient resources were allocated to the personnel security function to maintain new clearance requirements as well as clearance reviews. In some organisations, an increase in the volume of clearance requests has exacerbated this problem. Furthermore, in some organisations the shortage of resources coupled with responsibilities for other operational functions has hampered the security function and reduced its effectiveness in its primary roles.

19. The results of the audit highlight that management of personnel security needs to be improved in many respects to ensure compliance with the requirements of PSM 2000. Accordingly, many of the recommendations made in this report are designed to assist organisations to develop and adopt processes consistent with the requirements of the PSM.

20. As organisations implement the requirements of PSM 2000 and better practices are further disseminated across the Commonwealth public sector, the quality of vetting investigations and the personnel security process generally can be expected to improve. In addition, the increased oversight undertaken by the Protective Security Policy Committee (PSPC) through such mechanisms as the Commonwealth Protective Security Survey will assist this process.

Sound and better practices

21. The audit identified a number of examples of sound and better practices in the organisations reviewed. A summary of these is provided in Table 1.

Table 1
Sound and better practices

General management
Two organisations had formally considered their overall security risk environment, including the impact on personnel security.
Line managers were responsible for conducting position assessments for their area with the guidance, advice, and oversight of the security function.
Two organisations managed security assessment information using their Human Resource Management Information System (HRMIS) which provided improved security clearance management capability.
Pre-screening and employment
One organisation had a policy covering the requirement for pre-engagement checking and, if necessary, security clearances covering both its employees and contractors.
Two organisations had implemented formal processes to regularly monitor the security clearance requirements of contractors working on their 'accounts' under out-sourced arrangements.
One organisation had a policy requiring contracts to include clauses indicating contractors and/or their employees will be required to undergo a security assessment before commencement of the contract. In addition, the policy highlighted that contracts should warn of the possible lead-in times for obtaining clearances.
Assessment and decision process
One organisation has developed a pro forma referee report to provide guidance to subject referees on the relevant assessment areas.
Several organisations routinely appended a clearance work-sheet (or checklist) on file to record clearance actions and results.
Two organisations had developed specific questionnaires to further support and enhance the suitability assessment.
Maintenance, monitoring and review
Two organisations had integrated personnel security information with the HRMIS providing an effective management reporting capability and supporting the maintenance of clearances.
Two organisations periodically identified security clearances due for renewal.

Reports to organisations

22. Each of the organisations included in the audit was issued with a comprehensive management report providing conclusions against each of the audit criteria and detailed findings against the evaluation criteria, including recommendations for improvement, where necessary. The organisations have responded to the findings and recommendations presented to them and, where appropriate, advised of remedial action taken or proposed.

Recommendations

The nature of the issues raised in this audit have wide application across the Commonwealth. Accordingly, the following recommendations are considered to be applicable to all Commonwealth organisations with a personnel security requirement. Organisations should consider the recommendations in the context of PSM 2000 and the risks involved.

Policy

Recommendation No. 1 Para. 2.5–2.7

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.

Security Risk Management

Recommendation No. 2 Para. 2.8–2.9

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.

Position Assessments

Recommendation No. 3 Para. 2.10–2.14

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.

Contract Management

Recommendation No. 4 Para. 2.17–2.20

The ANAO ***recommends*** organisations adopt better practice contract management principles and standards in outsourced security clearance and vetting service arrangements. [6]

Documentation

Recommendation No. 5 Para. 2.43–2.47

The ANAO ***recommends*** organisations record all information collected during the course of a security clearance on the subject's Personal Security File.

Suitability indicators

Recommendation No. 6 Para. 2.48–2.52

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

Information management

Recommendation No. 7 Para. 2.61–2.67

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.

Security clearance reviews

Recommendation No. 8 Para. 2.68–2.70

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.

---

6 Refer to Australian National Audit Office, *Contract Management Better Practice Guide*, Commonwealth of Australia, February 2001. Available from http://www.anao.gov.au

Security awareness

Recommendation No. 9 Para. 2.71

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.

Security aftercare

Recommendation No. 10 Para. 2.72–2.73

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.

Audit Findings and Conclusions

1. Introduction

Background

1.1 Protective security concerns the protection of information, assets and human resources from potential threats. It includes physical security (eg, building access control), personnel security (eg, background investigations), information security (eg, classification of documents), and computer and communications security (eg, IT access controls). An effective and efficient protective security practice requires these elements to be complementary and for security measures to be applied in light of identified risks and the organisation's context. Furthermore, those people entrusted with protecting information and other resources must be suitable and meet high standards of integrity and honesty. That is, protective security also has an important ethical dimension, which should be shaped by the APS Values and Code of Conduct.

1.2 The Commonwealth Attorney-General is responsible for protective security policy, which is disseminated through the Commonwealth Protective Security Manual (PSM). As discussed in paragraph 1.12, the PSM has been endorsed by the Government. While individual Ministers are responsible for the implementation of protective security within their respective portfolios, in practice, responsibility for the day-to-day management of protective security processes in each Commonwealth organisation, lies with the head of the organisation. The Attorney-General's portfolio provides protective security support to the Commonwealth through the Australian Security Intelligence Organisation (ASIO) and the Protective Security Coordination Centre (PSCC).

1.3 Personnel security, including the security clearance process, is a valuable and essential element of managing the risk inherent in allowing Commonwealth and other personnel access to classified information. The central tenet of personnel security is that access to sensitive information is restricted to people with a legitimate requirement (ie. a 'need to know'), 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.

1.4 There is an increased exposure to security breaches and the associated costs and risks if the security clearance process is not conducted objectively and with consideration of current threats and risks. Personnel security and the security clearance processes should extend beyond comprehensive and informed checking and continued monitoring and review to include the rigorous assessment of clearance requirements and identifying organisation-specific risk factors.

1.5 A visible reminder of the important role of the personnel security and the security clearance process in particular and the need for continued vigilance are recent high-profile espionage cases.

1.6 For example, in one case in the United States of America, the subject was a long-term employee who had engaged in espionage activity for nearly ten years. The report of investigation[7] into the case suggests the matter might have been avoided or concluded earlier had there been a coordinated effort to officially evaluate a number of factors concerning the subject's continued suitability to access to sensitive information and an increasing vulnerability to potential espionage. These factors included chronic alcohol abuse, performance and suitability problems, several violations of personnel security rules, financial problems and unexplained changes in the financial circumstances and physical appearance of the subject.

ANAO Protective Security Audits

1.7 Protective Security Audits (PSA) are undertaken as part of the ANAO's Financial Control and Administration (FCA) program. This program is concerned with undertaking audits and making recommendations aimed at improving the quality of public sector administration and assisting organisations by identifying and reporting better practices.

Security clearance activity

1.8 The last 12 to 18 months have seen significant activity in relation to protective security in the APS, including personnel security. The following is a summary of the current environment in which personnel security operates in the Australian Public Sector (APS).

---

7 *The Aldrich H. Ames Case - Abstract of Report of Investigation*, Central Intelligence Agency, October 1994, United States of America.

1.9 There are two categories of security clearance, Designated Security Assessment Position (DSAP), which is used for positions requiring access to national security classified information[8], and Position of Trust (POT)[9], which is used for positions requiring access to non-national security information. A security assessment undertaken by the Australian Security Intelligence Organisation (ASIO) must be requested for all occupants of a DSAP. The appropriate level of clearance within these two categories is determined through an analysis by the organisation of the duties and tasks to be performed, including, but not restricted to, the level of access to security classified information required.

1.10 An accurate estimate of the number of security clearances undertaken in the Commonwealth is difficult to establish because there is no single, consolidated information source. The organisations included in the audit processed approximately 6600 DSAP and 1800 POT security clearances in 1999–2000. Since 1996–1997, the number of DSAP security clearances undertaken by Commonwealth organisations has increased; for example, from 11 467 in 1998–1999 to 12 179 in 1999–2000.[10] The cause of this increase is unclear; although, the Sydney Olympic Games security operation has accounted for some of the increase as has an increased awareness of personnel security due to recent high profile espionage cases.

Protective Security Manual

1.11 The Commonwealth Protective Security Manual (PSM) sets out the policies, practices and procedures organisations are required to follow to maintain an effective protective security framework. It confirms that an effective protective security environment is an essential element of good governance and sound business practice.

---

8 National security information is any official resource that records information about or is associated with Australia's security, defence, international relations or national interest. Refer to Attorney-General's Department, *Commonwealth Protective Security Manual*, Commonwealth of Australia, 2000, Part C section 6.

9 DSAPs are further classified as TOP SECRET, SECRET or CONFIDENTIAL; and POTs are further classified as HIGHLY PROTECTED or PROTECTED.

10 As indicated by the number of security assessment requests received by ASIO during the period 1998–1999 to 1999–2000. This figure also includes security clearance reviews requiring an ASIO assessment.

1.12 The content and presentation of the PSM has been subject to extensive review over the last few years. Following endorsement by the National Security Committee of Cabinet (NSC) in September 2000, the new PSM was officially launched in December 2000[11], replacing the 1991 edition. The Government has, on several occasions, emphasised the importance it attaches to protective security, particularly highlighting the importance of maintaining an effective level of security awareness and the measures included in the PSM to address this issue.

1.13 In addition to the endorsement of the Cabinet, another significant enhancement is that the new PSM contains a series of minimum standards for the conduct of protective security processes. Although heads of organisations are able, in limited circumstances, to issue waivers if a particular minimum standard is unable to be adhered to, these waivers are to be reported to the Secretary of the Attorney-General's Department and to the Auditor-General.

Contemporary issues

Inspector-General of Intelligence and Security's Inquiry into Security Issues

1.14 The Inspector-General of Intelligence and Security (IGIS) commenced an inquiry in 1999 to provide advice on measures to be taken to strengthen the protection of classified information against espionage. While the majority of the report's recommendations are targeted at organisations in the Australian Intelligence Community and the small number of organisations with access to highly sensitive intelligence and security material, it also identifies several issues relevant to the wider Commonwealth Public Sector.

1.15 Issues pertaining to all Commonwealth organisations which are designed to improve the level of accountability for effective security practices include the following:

- preparation of an annual report by the Protective Security Policy Committee (PSPC) assessing the status of protective security within the Commonwealth. To assist the PSPC meet this requirement, the inquiry considered organisations should advise the PSPC on the extent of their compliance with the PSM standards. The PSPC recently issued the *'Commonwealth Protective Security Survey—as at 30 June 2001'* to collect the information needed to satisfy this requirement;

---

[11] The new manual was launched by the Protective Security Coordination Centre (PSCC) in *Protective Security Bulletin (PSB) No. 6/00 of 7 December 2000.*

- organisations subject to a protective security audit by the ANAO are to inform the PSPC of the results of the audit and their responses to the findings of the audit; and
- PSM should be updated more regularly to keep pace with the changing security environment. To satisfy this recommendation the PSPC has implemented a program to review selected components of the new PSM each year. At the present time, reviews of Part D (Personnel Security) and Part B (Risk Management) are in progress.

Personnel Security Review

1.16 In 1999 the PSPC conducted a review to critically assess all aspects of personnel security management practices and to develop 'best practice' standards for the implementation and coordination of effective personnel security management. The review found security clearance processes were needlessly complex, inefficient, and cumbersome. Some of the concerns about the manner in which personnel security was being undertaken included:

- contradictory interpretations of guidance in the PSM had resulted in inconsistent security clearance practices leading to reciprocity problems, delays and increased costs;
- an excessive number of different forms in use;
- minimal use of automation to aid security clearance management; and
- lack of appreciation of risks to personnel security management.

1.17 The results of the personnel security review, including a draft replacement for Part D of the PSM, are currently being assessed by the PSPC in light of recent issues and a revised Part D is expected to be promulgated by the middle of 2002. The analysis, findings and recommendations of the personnel security review provided valuable background material for use in the development of the evaluation criteria for this audit.

Provision of Vetting Services by the Private Sector

1.18 Consistent with other Government functions, the provision of protective security services, including security clearances should be subject to a continual search for improved efficiency and effectiveness. One approach to performance improvement available to organisations is to assess the delivery of personnel security functions against suitable private sector service providers. The issue of the provision of personnel security services by the private sector was recently considered by the PSPC in Protective Security Bulletin (PSB) No. 1/01.

1.19 PSB No. 1/01 highlighted several aspects of the security clearance process which should remain the responsibility of the organisation and ought not to be required of private sector service providers. These roles include:

- identifying security clearance requirements;
- assessing security clearance recommendations;
- granting, denying or withdrawing security clearances;
- conducting Top Secret (positive vetting) security clearances; and
- retention of Personal Security Files (PSFs).

Accreditation of Security Clearance Service Providers

1.20 Allied to the use of the private sector service providers to undertake security clearances is the issue of whether, and how, organisations might assess the capacity and capability of these providers. The onus is on each individual organisation to ensure private sector providers engaged to provide vetting services satisfy the minimum standards of the PSM.

1.21 Some of the considerations involved in an assessment of capability may include whether the private sector service provider:

- meets the minimum standards in relation to physical and IT security;
- has staff with the requisite security clearance and who have undertaken appropriate training (training requirements are discussed further in paragraph 1.24);
- has a quality assurance framework in place; and
- has mechanisms in place to deal with under-performance.

1.22 A logical extension of this process suggests all security clearance service providers should be accredited or at least measured against a set of minimum parameters or standards. The Personnel Security Review conducted by the PSPC (paragraph 1.16) considered standards should be developed and used for all service delivery arrangements. These standards should cover fully in-house security clearance activity, organisation-sponsored arrangements (such as the Australian Security Vetting Service) or any other arrangement when security clearance work is undertaken outside of the organisation's premises (including working from home).

Personnel Security Training

1.23 To ensure the effective conduct of the security clearance process, each organisation must provide the appropriate level of training to those staff who manage and implement personnel security policies. This view is reinforced by clause 3.10 of the new PSM which indicates that anyone undertaking security clearances on behalf of the Commonwealth must have appropriate training in protective security policy and practice in general, and personnel security processes specifically.

1.24 The PSCC, through its training centre, provides a series of training courses to ensure those involved in personnel security are provided with requisite knowledge and skills to conduct security clearances. The NSC has endorsed the PSCC Training Centre as the provider of protective security training, including personnel security training for staff in, and contractors to, the APS. Clause 3.18 in Part D of the new manual indicates that people who have not undertaken this training or similar training recognised by the PSCC must not conduct security clearances in Australia.

2. Audit Findings

Introduction

2.1 This chapter discusses the audit findings and recommendations under the following four headings:

- General management;
- Pre-screening and employment checking;
- Assessment and decision processes; and
- Maintenance, monitoring and review.

2.2 These four areas are central elements in the effective management of the personnel security function, including security clearances.

2.3 The audit results are presented in two distinct categories: audit findings and recommendations, and sound and better practices. The audit findings detail compliance or process issues that affect the efficiency and effectiveness of organisation's personnel security. Sound and better practice observations relate to business practices which, if adopted, would strengthen personnel security management and lead to improved effectiveness and efficiency.

Audit findings—General management

Introduction

2.4 Personnel security processes should occur within, and be influenced and supported by, an informed framework reflecting the organisation's operations, as well as Commonwealth protective security policy. In essence, the aim of this part of the audit was to assess the management and control framework of personnel security within each organisation.[12] The audit found scope for improvement in all organisations, particularly in the areas of security risk management and security policy. The evaluation criteria were grouped into the following components:

- *Policy and procedures:* Organisation security policy and procedure documents clearly outline personnel security delegations, policy decisions, and processes in line with PSM requirements.

---

[12] The control framework provides an important link between an organisation's objectives and the functions and tasks to achieve those objectives. For more detail on the components of the control framework refer to Australian National Audit Office, *Controlling Performance and Outcomes,* Commonwealth of Australia, 1997. Available from http://www.anao.gov.au

- *Security risk management:* Formal risk assessments are the basis for evaluating the costs and benefits of controls and assist the organisation to apply consistent and defensible treatments to identified threats and risks. Implementation of risk assessment processes should be a key part of effective personnel security management.
- *Position assessments:* The number of security clearances is kept to a minimum and each DSAP/POT is determined by an analysis of the duties and tasks to be performed.
- *Quality control:* Management and control processes provide reasonable assurance of the efficiency and effectiveness of personnel security outcomes. This includes such elements as contract management processes, clearance turn-around times, audit processes, and accountability.

Policy and procedures

Table 2.1

Principle
Security policy and procedure documents clearly outline personnel security delegations, policy decisions, and processes in line with PSM requirements.
Evaluation criteria
Personnel security policy and procedures have been developed and comply with the PSM.
Audit findings
In relation to the six organisations reviewed, the audit found: • two organisations relied on the PSM in place of organisation-specific policy and procedures; • policy and procedure documents in two organisations were too detailed and prescriptive; and • inconsistent policies and practices in organisations with a regionalised security function.

2.5 Better practice is the promulgation and maintenance of sound security policies and procedures that reflect the organisation's specific environment and circumstances. The existence of organisation-specific policies and procedures assist in the overall acceptance and ownership of security principles and their integration into the organisation's broader management and operational activity. The release of PSM 2000 is an opportune time for organisations to review security policy and procedures to ensure they continue to reflect their operating environment and PSM requirements accurately.

2.6 Each of the organisations reviewed had developed protective security policy and procedures. However, with the exception of two organisations, the audit found there was scope for improvement to enhance the effectiveness and useability of that policy and procedural documentation to personnel security. For example, two organisations relied almost exclusively on the PSM and had not developed organisation-specific personnel security policy and procedure instruments to formally adopt and supplement as appropriate the requirements of the PSM. While at the other extreme, two organisations had promulgated policy and procedural manuals that were too detailed and prescriptive resulting in a lack of procedural flexibility.

2.7 The audit noted inadequate policy and procedure statements contributed to inconsistent personnel security practices. This was particularly the case for those organisations with a regionalised security function. Many of the issues found during the audit and discussed in this report could have been avoided through a more effective governance, accountability, and audit framework supported by clear personnel security policy and procedure statements.

Security risk management

Table 2.2

Principle
Risk assessment processes are an essential part of effective personnel security management and assists in the application of consistent and defensible treatments to identified threats and risks.
Evaluation criteria
Security Risk Assessments should be current, reflect the current security context and inform the security clearance process.
Audit findings
In relation to the six organisations reviewed, the audit found: • a lack of security risk management processes and practices; • security risk management processes not integrated effectively with the broader organisational risk management framework; • limited coverage of personnel security issues in existing protective security risk assessments; and • no clear links between risk factors and clearance suitability assessments.
Sound and better practices
The following sound and better practice was noted: • two organisations had formally considered their overall security risk environment, including the impact upon personnel security.

2.8 Effective personnel security involves assessing both the subject and the environment in which the subject will be employed. Therefore, knowledge of potential risk factors, their consequences, and the development of strategies to mitigate these risks are essential to the effectiveness of personnel security procedures and policies. A risk management approach enables more focussed and context-specific personnel security and supports more efficient and effective resource allocation and policy formulation. The PSM outlines the principles for effective security risk management and depending on the type of exposure, the security clearance process detailed in the PSM provides an effective process to treat identified security risks.[13]

2.9 The audit found a need for improvement in the integration of threat/risk management processes within the personnel security function in four of the six organisations audited. While each of the organisations had established risk management frameworks, these were often limited to operational or program delivery matters and did not extend to protective security or other corporate functions. Only two organisations had formally considered their protective security risk environment. However, at the time of the audit these two organisations had not fully assessed how the risk factors identified might be reflected in, or used to inform personnel security practices, including the conduct of security clearances and the assessment of suitability. In the absence of a risk assessment, it is difficult to objectively assess protective security policies and practices, as each organisation will face different threats according to its mandate and sphere of operations.

[13] Attorney-General's Department, op. cit. Part B.

Position assessments

Table 2.3

Principle
Security clearances are kept to a minimum and determined by an analysis of the duties and tasks to be performed in each position, role, or function.
Evaluation criteria
• DSAP/POT assessments reflect the duties and tasks of the position and the organisation's risk profile. • Clearance requirements should reflect the organisation's roles, positions and classified material holdings. • Access to classified information without adequate clearance should comply with PSM guidelines.
Audit findings
In relation to the six organisations reviewed, the audit found: • line managers lacked knowledge of assessment criteria for DSAP/POTs, and consequently assessments in some instances were either not conducted or were arbitrary; • two organisations with a blanket, or minimum security clearance policy lacked a clear policy statement to support this; and • the management of DSAP/POT information did not adequately support the review and management of organisation clearance requirements.
Sound and better practices
The following sound and better practices were noted: • line managers were responsible for conducting position assessments for their area with guidance, advice, and oversight of the security branch; and • two organisations managed position assessment information using their Human Resource Management Information System (HRMIS) providing improved security clearance management capability.

2.10 Personnel security involves restricting access to classified information to those individuals with a legitimate need to know and who are assessed as suitably responsible and trustworthy. This requires organisations to assess, on an ongoing basis, those tasks and duties that require the occupant of a position to have access to classified material and therefore a security clearance.[14] In addition, certain positions within an organisation, while not necessarily requiring frequent access to classified material, nonetheless, involve a high degree of trust and accountability, for example IT positions. Position assessments can also ensure the efficient use of personnel security resources by ensuring the clearance level is not excessive for the position.

[14] Attorney-General's Department, op.cit. Part D, paragraph 5.23.

2.11 At the time of the audit only one organisation had effective processes in place over the conduct of position assessments. At a further three organisations, the audit found some scope for improvement in the management of position assessments. Two organisations did not conduct position assessments.

2.12 The audit found that line managers often initiated requests for security clearances without sufficient consideration or assessment of the need. Consequently, in these instances it was difficult to assess whether the organisation's DSAP/POT classifications were appropriate. Although the security area in each organisation was involved to varying degrees with the determination of DSAP/POT levels, there was some room for improvement in this area. In particular, for example, by providing guidance on assessments and establishing controls to enable the quality (and completeness) of decisions to be assessed.

2.13 A crucial element in effective personnel security management is the management of information to support the maintenance and review of position security assessments. Two organisations were unable to readily produce details on the number and/or status of existing DSAP/POTs and not all organisations had effective processes to ensure the periodic review of existing DSAP/POTs. In addition, the audit found discrepancies between the number of security assessed positions and the actual number of staff with security clearances. Although this latter situation may provide some flexibility in staff management practices, the maintenance of uniformity between the number of security assessed positions and the actual number of security clearances is consistent with better practice.

2.14 Two organisations had minimum clearance policies in response to a specific organisation risk. In this context, the conduct of individual position assessments is neither practical nor necessary as the minimum clearance requirement negates the need. However, neither organisation had an adequate policy statement outlining the requirement and justification for a blanket minimum clearance, or clarification that any position requiring a clearance above the minimum level must be supported by an appropriate assessment.

Quality control

Table 2.4

Principle
The management and control framework is appropriate and provides reasonable assurance of the efficiency and effectiveness of personnel security outcomes.
Evaluation criteria
• Quality Control processes are in place to ensure early identification of errors or problems. • Cost and efficiency controls are in place and monitored effectively.
Audit findings
In relation to the seven organisations reviewed, the audit found: • five organisations had a significant backlog of security clearances, and all were experiencing long delays in processing security clearance applications; and • while those organisations using external service providers were generally happy with the level of service provided, the audit found ineffective performance standards in service agreements and limited review or monitoring of performance.

Clearance backlog

2.15 Two of the more pressing personnel security issues facing the organisations in the audit were the lengthy delays often encountered undertaking security clearances and the associated backlog in the number of clearances being, or awaiting processing. In the organisations audited, 79 (64 per cent) of the security clearances reviewed took longer than two months to process, 58 (46 per cent) of these clearances took longer than three months and 21 (18 per cent) took longer than six months. At the time of the audit the estimated backlogs in the organisations audited ranged from around 10 cases (6 per cent of the total security clearances processed in 1999–2000) up to over 2000 cases (representing 55 per cent of the security clearances processed in 1999–2000). The reasons for the delays and the associated backlog suggested by the organisations varied, but included a lack of resources; increased clearance requirements; and delays obtaining external evidence. Not all of these causes are within the direct control of the organisation. Most significantly, at the time of the audit, organisations faced at least a three-month delay obtaining a security assessment[15] from ASIO.

[15] A security assessment is required from ASIO for all DSAP security clearances (refer Attorney-General's Department, op. cit. Part D, section 7).

2.16 Although the audit did not examine ASIO's security assessment process, ASIO provided comments on the causes for this delay. The Sydney Olympic security operation significantly increased ASIO's security assessment workload,[16] and there has also been an increase in the number of cases classified as 'complex' and, as such, requiring additional investigation. The increase in 'complex' cases is because of an increase in the number of clearance requests where aspects of the subject's background were unable to be readily or easily checked.

Contract management

2.17 While the PSM does not contain any specific advice or guidance to organisations on the use of private firms, there are currently no legal or policy restrictions precluding organisations from engaging private sector providers to conduct elements of the security clearance process. In this regard, organisations are free to evaluate the desirability or otherwise of outsourcing elements of personnel security.

2.18 While the responsibility to perform functions or services may be transferred to the private sector, accountability for the organisation's security arrangements cannot. Given the potential risks involved, sound contract management is vital to ensure service providers operate at a consistently high standard and in accordance with the minimum standards in the PSM.

2.19 The audit found several areas for improvement in relation to service agreements and the management of service performance. Perhaps most importantly, the audit found insufficient performance measurement in the organisations using external service providers. For example, although agreements required providers to perform services to a high standard using due skill, the required standards of performance were not clearly defined. In addition, organisations required more formal processes to actively manage service delivery arrangements to ensure consistent quality and a cost-effective service. For example, although provision was made in service delivery agreements to do so, organisations had not conducted a review of the service. In addition, organisations did not have formal quality assurance processes to assess the security clearance recommendations made by the service provider.

---

[16] The Olympics accreditation workload was 62 237 assessments as of 30 June 2000. Refer to ASIO's Annual Report to Parliament 1999–2000.

2.20 The audit also found there was limited formal monitoring of whether providers were meeting 'turnaround times' outlined in the service agreement. The audit found that, on average, vetting service providers were taking longer to complete security clearances than the common standard of six weeks. The average elapsed time taken per security clearance by one service provider during 2000–2001 was approximately 11 weeks.

Conclusion—General management

2.21 The issues identified reflect inadequate security-related governance and control arrangements, including the application of risk management principles within organisations. Effective personnel security arrangements, like protective security generally, requires the commitment and support of senior management.

2.22 Overall, organisations could benefit from increased management oversight and involvement in personnel security, particularly in the area of risk management, security policy, and audit processes. More specifically, this includes implementing contract management better practice, more rigorous risk management processes and practices, and the integration of protective security into broader organisation operations.

Recommendation No.1—Policy

2.23 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.

Implementing the recommendation

2.24 The PSM is a broad statement of Commonwealth policy and should be used as a reference, not a replacement, for individual organisation policy and procedures. The lack of adequate policy and procedure documents may lead to vetting practices and procedures being inconsistently applied and/or organisations not complying with PSM standards. Further, without documentation, much of the understanding of the organisation's risk environment, vetting procedures, and corporate knowledge may be lost through staff turnover. In addition, the lack of organisation-specific policy and procedures presents difficulties in ensuring staff are properly informed and aware of their protective security responsibilities.

2.25 Given the comprehensive nature of the PSM, organisation-specific protective security policy and procedure documents generally need only comprise relatively brief and succinct policy statements with a reference to the PSM for more detail, where required. The following table provides some suggestions of content for consideration:

Table 2.6
Personnel security policy and procedure considerations

Corporate security policy
• A clear statement of any 'blanket' clearance requirement policy, including the supporting rationale • Access control policies, for example the off-site accommodation arrangements • Procedures for reporting contact with foreign officials • Reporting changes of circumstance • Guidance for staff on personnel security policy and procedure as required
Security Section Procedures
• Any standards or procedures to be applied in excess of PSM minimum requirements • Clearance documentation requirements • Re-validation procedures on transfer of clearance from another organisation • Organisation-specific suitability indicators • Any other strategies designed to achieve corporate security outcomes

Recommendation No.2—Security Risk Management

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.

Implementing the recommendation

2.26 Security risk management processes should be informed by broader risk management activity in the organisation. Security clearance processes should be undertaken in light of the assessment of the security risks faced by the organisation and informed by other relevant organisational activity. For example, DSAP/POT assessments should include consideration of the nature of possible security threats. A comprehensive and up to date Security Risk Assessment, covering all aspects of the security function, should be a key source of information in the design of the security clearance process.

Recommendation No.3—Position Assessments

2.27 The ANAO ***recommends:***

- registers of DSAPs/POTs 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.

Implementing the recommendation

2.28 Line managers should be responsible for the assessment of security clearance requirements and the maintenance of DSAP/POT lists in their areas of responsibility. To ensure consistency in assessments, the security section should provide guidance, advice and put in place a quality control process. This approach would aid the integration of personnel security practices into general organisational management practices.

2.29 The integration of position assessment information with the organisation's existing HRMIS or other appropriate corporate system would improve capability in this area (this is discussed further in Maintenance, Monitoring and Review below, and also in Recommendation No.7).

Recommendation No.4—Contract Management

2.30 The ANAO ***recommends*** organisations adopt better practice contract management principles and standards[17] in outsourced security clearance and vetting service arrangements.

Implementing the recommendation

2.31 To ensure the standards of service delivery remain appropriate to organisational needs and expectations, better practice contract management includes the following:

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

---

[17] Refer to Australian National Audit Office, *Contract Management Better Practice Guide*, Commonwealth of Australia, February 2001. Available from http://www.anao.gov.au

2.32 Contracts should also include requirements for the protection of personal information and compliance with the Information Privacy Principles. This should include reference to specific measures or minimum information management standards of protection, for example the use of secure containers, information handling requirements, and the need to encrypt information held on electronic storage devices. If a subject's information is to be held on the contractor's premises, periodic inspections should be conducted to confirm these minimum standards are met.

2.33 To ensure clearance recommendations are appropriate and reflect both the organisation's personnel security requirements and the principles of natural justice, some clearances cannot be completed within a standard timeframe. If performance measures concentrate solely on minimum turn-around time, there is a possibility the quality of service will suffer. Finally, because the external service provider will not have the benefit of the organisation's corporate knowledge, agreements should include the use of organisation-specific risk factors and details of other organisation-specific vetting requirements.

Audit findings—Pre-screening and employment

Introduction

2.34 Personnel security eligibility standards and access restrictions should be appropriate to the organisational context and consistent, thus supporting effective personnel security practices and enhancing clearance portability. This is the basis of the maintenance of good security across the Commonwealth as a whole.

Table 2.7

Principle
In addition to fulfilling the standards and procedures for recruitment in the Commonwealth, pre-screening and employment checks should ensure eligibility criteria, waivers, and temporary access controls are sound and comply with the PSM.
Audit evaluation criteria
• Contractors require a security clearance appropriate to their access • Eligibility waivers are granted in accordance with PSM guidelines • Organisations recognise clearances from previous organisations and allow portability of clearances • Pre-employment screening should be conducted according to PSM guidelines

continued next page

Audit findings
Generally, organisations were found to have effective procedures in place covering pre-screening and employment requirements. Each of the six organisations reviewed met these criteria.
Sound and better practices
The following sound and better practices were noted during the audit: • one organisation had a policy covering the requirement for pre-engagement checking and, if necessary, security clearances covering both its employees and contractors; • two organisations had implemented formal processes to regularly monitor the security clearance requirements of contractors working on their 'accounts' under out-sourced arrangements; and • one organisation had a policy requiring contracts to include clauses indicating contractors and/or their employees will be required to undergo security assessment before commencement of the contract. In addition, the policy highlighted that contracts should warn of the possible lead-in times for obtaining clearances.

Conclusion

2.35 The audit also examined the application of eligibility criteria, contractor clearances, access restrictions, portability, and the integration of personnel security management with organisation recruitment practices. All organisations in the audit met the evaluation criteria.

2.36 One of the primary factors in improving the effectiveness of this aspect of personnel security is the interconnection between the security function and the human resource function in the organisation. The requirement to hold a security clearance should be clear throughout the recruitment phase and much of the information supporting the vetting process is, or can be, collected during the initial recruitment phase.[18] Closer cooperation between the security function and human resource function should also promote an increased awareness of personnel security issues. Those organisations where the security function is either integrated or closely aligned with the human resource function had fewer problems in managing the security clearance requirements of new or prospective staff.

2.37 Another pertinent contemporary issue is the transfer of an individual's security clearance between Commonwealth organisations, commonly known as 'portability'. The main benefits of 'portability' are a reduction in unnecessary duplication in security clearance activity, reduction in costs and delays and increased efficiency. The 'portability' of security clearances in large part, depends on the respective organisations' compliance with the PSM's minimum checking standards.

[18] Recruitment in this context also includes the recruitment and management of contractors.

2.38 Each of the organisations audited accepted the principle of security clearance portability and had instituted procedures requiring the review of clearances previously provided by other Commonwealth organisations. As a rule, organisations checked the quality of clearances and assessed whether the clearance met the organisation's standards or if further information needed to be sought. Better practice noted in one organisation was that clearances from other organisations were assessed against risk factors specific to that organisation before they were accepted.

Audit findings—Assessment and decision processes

Introduction

2.39 The principal aim of the vetting process is to ensure individuals with access to classified or sensitive information can be relied upon to properly use and protect that information. Consequently, when considering whether to grant a clearance the organisation must have enough information to be reasonably assured of the subject's maturity, trustworthiness, responsibility, honesty, and loyalty given the nature of the subject's prospective position and the organisation's risk environment. This suitability is determined through investigation of the subject's character, relevant attributes, background, and actions.[19]

2.40 The audit examined the efficiency and effectiveness of vetting and assessment processes, and assessed compliance with the PSM. The audit findings in this section are summarised under the following evaluation criteria:

- *Documentation:* Information collected in the initial security clearance package and generated by the vetting investigation provides the foundation for the suitability assessment, clearance decision, quality assurance, and future reviews.
- *Suitability assessment:* Adequate and comprehensive information collection, collation, and analysis should support the assessment of clearance suitability. In addition, it should reflect the organisation's threat/risk environment.

[19] Attorney-General's Department, op. cit. Part D, section 6.

Documentation

Table 2.8

Principle
Information collected in the initial security clearance package and generated by the vetting investigation provides the foundation for the suitability assessment, clearance decision, quality assurance, and future reviews.
Evaluation criteria
• Security packages include, at a minimum, the information and forms outlined in the PSM. • Subjects are fully informed of the security clearance process and of their rights and obligations. • Sufficient and relevant documentation should be retained on the subject's Personal Security File (PSF). • Background checks and the assessment process complies with the PSM in regard to the minimum checks, standards and principles. • Subject and referee interviews are conducted in accordance with the PSM. • Security clearance decision complies with PSM guidelines.
Audit findings
In relation to the seven organisations reviewed, the audit found: • the security clearance packages used in each organisation largely met the minimum PSM requirements. They could be enhanced however, through the inclusion of information on post-clearance responsibilities; and • there was scope for improvement of documentation in three organisations. Primary issues were: — limited or no record of clearance actions and their outcome; — records of interview did not adequately record salient information; and — incidents relevant to suitability were often not retained on the PSF.
Sound and better practices
The following sound and better practices were noted: • one organisation has developed a pro forma referee report to provide guidance to subject referees on the relevant assessment areas; and • several organisations routinely appended a clearance work-sheet (or checklist) on file to record clearance actions and results.

2.41 The security clearance packages used by each of the seven organisations audited met the minimum requirements of the PSM, with the exception that none of the organisations included information on the clearance subject's post-clearance responsibilities. The provision of the package presents a useful opportunity to inform the subject of the ongoing responsibilities of holding a security clearance and to commence the security awareness and education process. Examples of the information which should be provided includes reporting changes of circumstance, clearance review requirements, and contact reporting.

2.42 By providing this information in the security clearance packs, the organisation does not transfer or diminish its responsibility for post clearance maintenance. However, it will assist clearance subjects to gain a fully informed understanding of what is involved in obtaining and holding a security clearance.

2.43 Adequate documentation including a record of clearance actions, interview reports, referee reports, and security incident reports are essential not only for current clearance action, but also to support future activity, including periodic reviews and quality assurance reviews.[20]

2.44 Two organisations did not undertake adequate quality control of the clearance process and this resulted in inadequacies in the standard of interview reporting. For example, the audit found instances of interview aides-mémoire comprising single word answers appended to the PSF as the record of interview. Although the interview aide-mémoire is a necessary guide to conducting security interviews, it should not be used to replace the preparation of a summary interview report with the vetting officer's analysis and conclusions.

2.45 In three organisations there was often no record of clearance checks and their outcomes, and limited or no record of referee reports when these were not provided in writing. Consequently, at times, it was difficult to establish whether the required minimum checks had been completed. An additional issue arising from the above practice is that at the time a PSF is transferred to another organisation, lack of information on the file can impede the ability of the receiving organisation to accept the existing clearance.

2.46 Further, many referee reports observed during the audit were considered to be of limited use in assessing suitability because they were often written as an employment style reference, or the referee was not aware of the clearance process and assessment factors. To address this, one organisation had developed a pro forma referee report with specific questions to guide referee's responses. The ANAO considers this practice significantly improved the value of referee reports in the suitability assessment process because it ensured referees focussed on security issues rather than job skills.

---

[20] Attorney-General's Department, op. cit. Part D Section 11 contains matrices of minimum document and clearance action requirements.

2.47 The utility of information reflecting a subject's suitability does not end with the approval of the clearance. An important component of the aftercare process[21] is the continued monitoring of changes, events, and other factors affecting continued suitability. Consequently, documentation on the PSF should include security incident reports and other relevant information. Although five of the organisations had some form of security incident reporting, there was limited indication that incidents were routinely recorded on the subject's PSF, where appropriate. The result is that information relevant to continued suitability might not be considered during the next clearance action.

Suitability assessment

Table 2.9

Principle
Comprehensive information collection, collation, and analysis should support the assessment of clearance suitability. In addition, it should reflect the organisation's threat/risk environment.
Evaluation criteria
• Assessment of suitability complies with the PSM. • Vetting assessment reflects current and relevant risk factors.
Audit findings
In relation to the seven organisations reviewed, the audit found: • five organisations had not identified organisation-specific suitability indicators to supplement the generic PSM indicators; and • there was little evidence of the explicit application of suitability indicators to the analysis of suitability.
Sound and better practices
The following sound and better practices were noted: • two organisations had developed specific questionnaires to further support and enhance the suitability assessment.

2.48 The assessment of suitability is central to the security clearance process. The PSM outlines a number of generic indicators of behaviour or history that may demonstrate clearance suitability or conversely limited susceptibility to compromise. Although these indicators can usefully inform the clearance process, by refining these generic indicators suitability assessments can be targeted towards, or more focused on, the organisation's business and any potential risk factors in the organisation's environment.

---

[21] See further discussion on aftercare under *Maintenance, Monitoring and Review* below.

2.49 In addition, the development of organisation-specific indicators provides a more effective and rigorous means of guidance, particularly for staff less experienced with the organisation's business and risks. Several organisations held the US Adjudicative Desk Reference (ADR)[22] within the security section; however, it appeared to be rarely used and had not been integrated into the suitability assessment. The ADR, although tailored to the US context, nonetheless provides additional and more specific guidance to the suitability assessment.

2.50 Although all organisations in the audit demonstrated an understanding of the generic suitability factors contained in the PSM, most were unable to demonstrate they explicitly applied these factors during the clearance process. Rather, suitability in most organisations was assessed through the experience of its vetting staff and their knowledge of organisation-specific suitability issues.

2.51 One argument against the use of organisation-specific suitability indicators is that it may impede the portability of security clearances between organisations. However, such indicators should not replace, but rather supplement the generic PSM indicators. If the receiving organisation conducts a quality assurance review or revalidation there would be no impact upon clearance portability; to the contrary, it is likely that assurance in the quality of clearances will increase as a result of the additional indicators.

2.52 Three organisations had developed and implemented specific questionnaires to address particular areas of concern identified either during the vetting investigation or related to the organisation's area of operation. For example, one organisation administers a '*Substance Abuse*' questionnaire where the vetting investigation indicates some level of substance use. This is an improvement on PSM minimum standards and supports a more balanced and considered suitability assessment, particularly considering such questionnaires often reveal evidence or information that would not otherwise be obtained.

---

[22] The ADR is a compendium of background information and reference material on behaviour relevant to clearance suitability designed to assist security personnel in making informed judgments on personnel security. It was developed by the Security Research Center, US Defense Security Service and is available from http://www.dss.mil.

Conclusion

2.53 Overall the audit found security clearance assessment processes to be undertaken objectively and largely in compliance with the standards contained in the PSM. A number of issues identified during the audit, however, pose a risk to the continued effectiveness of these processes. The most significant of these were shortcomings relating to interview practices, maintenance of documentation and the tailoring of the suitability assessment to the organisation risk environment. The assessment of suitability to hold a security clearance is a cornerstone of the personnel security process and better practice is to focus the investigation and assessment on those factors most relevant to the organisation's risk environment.

2.54 In addition, it is equally important in terms of supporting the clearance decision process, future clearance activity, and the principles of natural justice, to adequately document and record all actions and information relevant to the vetting investigation.

Recommendation No.5—Documentation

2.55 The ANAO ***recommends*** organisations record all information collected during the course of a security clearance on the subject's Personal Security File.

Implementing the recommendation

2.56 The information recorded should include complete and accurate interview reports for each clearance interview as well as a summary outlining key issues and conclusions. In addition, the following information should be appended to the PSF to support quality assurance activity, clearance portability, and future clearance reviews:

- records of conversations;
- communication with referees or others relevant to the vetting procedure;
- a record of vetting actions and outcomes (for example a clearance action worksheet); and
- post-clearance security incident reports.[23]

[23] Attorney-General's Department, op. cit. Part D, section 10 provides guidance on the administration of personnel security records.

Recommendation No.6—Suitability indicators

2.57 The ANAO ***recommends*** organisations develop suitability indicators for use in security clearance assessments which are informed by organisation-specific risk/threat factors.

Implementing the recommendation

2.58 Organisation-specific suitability indicators should be derived from the generic indicators outlined in the PSM (Part D Section 6) and to fully exploit the effectiveness of any additional indicators or questionnaires, they should be supported by guidelines to assist in their consistent application. For example, guidelines might be designed to assist vetting officers recognise those circumstances when further action is required for a given response and to describe how and when responses should be used to corroborate or confirm information from other sources. Guidelines on suitability indicators should be included in the organisational policy and procedure documents as outlined in Recommendation 1.

Audit findings—Maintenance, monitoring and review

Introduction

2.59 The audit also examined the administration of security records to ensure the maintenance and review of security clearances is effective and consistent with Commonwealth policy requirements. The granting of the initial clearance is not the end of the personnel security cycle. Continued maintenance (commonly referred to as 'aftercare') includes security awareness and education programs, ongoing surveillance, and clearance reviews. To be effective, 'aftercare' needs to be supported by sound information management practices.

2.60 The audit findings in this section are summarised under the following headings:

- Information management: The efficient administration of PSFs, information management, and development of management reporting processes provide the foundation for effective clearance maintenance, monitoring, and review.
- Clearance reviews: Security clearances are appraised and re-evaluated according to the PSM criteria.
- Security education and awareness: A security culture effected through awareness and education programs is essential to the maintenance of effective personnel security.

Information management

Table 2.10

Principle
Efficient information management and management reporting processes provide the foundation for effective clearance maintenance, monitoring, and review.
Evaluation criteria
• Security clearance records administration and management complies with the PSM. • Access to Personnel Security Files should be strictly controlled.
Audit findings
In relation to the six organisations reviewed, the audit found: • four organisations had ineffective information management which restricted management reporting capability and the ability of managers to monitor security clearance status.
Sound and better practices
The following sound and better practice was noted: • two organisations had integrated personnel security information with the HRMIS providing an effective management reporting capability and supporting the maintenance of clearances.

2.61 The ANAO considered that the management of security information in four of the organisations was in need of improvement. For example, organisations did not always maintain information which the audit considered was useful to support the management of their personnel security function (including for example, details of position assessments, clearance review due dates, details of clearances in progress, costs of security clearances and lists of personal security files). More significantly, however, at the time of the audit three organisations did not have effective information management capabilities.

2.62 The major shortcoming identified in the audit was the limited capability within the organisations audited to support personnel security management through management reporting. For example, although one organisation had effective procedures for the assessment of security clearance requirements, it was unable to provide the number of DSAPs and POTs at each security clearance level. In addition, the problem with outdated clearance reviews (see discussion below) was exacerbated in several organisations due to the inability to monitor and report on clearance status. This was also a key finding in the last protective security audit – it found a general lack of consolidated management information on security assessed positions, the occupants of these positions, and the level and currency of their clearance.

2.63 Given the interrelation of personnel security and human resource information, better practice is to integrate personnel security information into the organisation's HRMIS[24] thereby supporting management reporting and access to security clearance information by line managers when required. Only two organisations in the audit did this; the others had developed stand-alone databases or other limited solutions. In two other organisations, one of the reasons noted for lack of integration with the HRMIS was the capability to record personnel security information had been lost during the transition to a new HRMIS. In these organisations, the ANAO was advised that the security function was not effectively consulted during the HRMIS planning and implementation phases.

2.64 The need for accurate information on the cost of the personnel security process is also particularly important given the emergence of external vetting service providers. The lack of an adequate information management capability limits the ability of organisations to assess the cost-effectiveness of its security function. Accurate cost information allows organisations to measure their financial performance against the cost of external services to assist them in assessing whether they are operating in a cost-effective manner.

2.65 In those organisations with some level of security information management, there were often problems with the accuracy of the records. For example, in one organisation, more than half of the personnel security records belonged to staff who were no longer employed by the organisation. In addition, many records had not been updated with changes in circumstance or other relevant information. The extent of the problem indicated this was a symptom of a broader lack of quality control and information maintenance.

2.66 In one organisation with a regionalised security function, local and non-networked information management systems had been developed to capture regional information. This resulted in information being unavailable more broadly across the organisation and the development of inconsistent data formats. While stand-alone databases are an acceptable response to managing security information in the absence of an organisation-wide solution, they limit security management capability, particularly in relation to managing security clearance reviews.

2.67 A further consequence of inadequate information management processes is a reduced capability to manage PSF holdings. Four organisations had files that were outside of the archival or destruction periods contained in Part D, section 10 of PSM 2000.

---

[24] See also the discussion regarding position assessments under *General Management* above.

Clearance reviews

Table 2.11

Principle
Security clearance reviews can be as, or more important than the initial clearance as circumstances may change and events may occur that significantly affects continuing suitability.
Evaluation criteria
Security clearances are appraised and re-evaluated according to the PSM.
Audit findings
In relation to the six organisations reviewed, the audit found: • five organisations had a significant backlog of outstanding clearance reviews, and four of these did not demonstrate the capacity, given existing resources and management, to overcome the backlog and effectively maintain the existing clearance review process.
Sound and better practices
The following sound and better practice was noted: • two organisations regularly identified security clearances due for renewal.

2.68 The evidence collected and assessments made at the time of granting a security clearance are necessarily largely, if not entirely, based on information about the clearance subject's background up to that time. Over time, personal or environmental circumstances and events will give rise to new factors which may impact on security clearance assessments. Overall, the audit has revealed much of the emphasis in personnel security management has been placed on the conduct of initial clearances, at times to the detriment of post clearance management, re-assessment and monitoring activities. The currency of security clearances can only be guaranteed through the conduct of regular clearance review and reappraisal processes that assess the continued suitability of individuals to hold the security clearance they have been granted.

2.69 A critical shortcoming, and one highlighted by more stringent requirements in the new PSM, is the significant level of overdue clearance reviews. The PSM requires security clearances to be reviewed at certain intervals.[25] Five organisations had officers occupying positions with security clearances that were outside these timeframes. Of particular concern also was that, four organisations did not have the capacity, given

[25] Not exceeding five years for SECRET, TOP SECRET & HIGHLY PROTECTED. Clearances not re-evaluated within six years lapse, and access should be denied until re-evaluation is complete. In addition, the minimum requirement for revalidation of TOP SECRET clearances is every 30 months.

their current resource levels and management practices, to effectively manage the security clearance review process and overcome the backlog. Additionally, they lacked the ability to monitor and report on clearance status because of inadequate information and business processes.

2.70 Although exact details were difficult to obtain because of shortcomings with available management information, the proportion of out-of-date security clearances in the organisations audited was estimated to range 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). In one organisation, around 50 per cent of all active Top Secret and Secret clearances were estimated to be out-of-date. Given the new PSM prescribes that Secret, Highly Protected, and Top Secret security clearances not re-evaluated within six years of the last vetting investigation will lapse, some organisations are facing a major challenge.

Security education and awareness

Table 2.12

Principle
A security culture effected through awareness and education programs is essential to the maintenance of effective personnel security.
Evaluation criteria
Personnel security maintenance and awareness is integrated into day to day organisation management.
Audit findings
In relation to the six organisations reviewed, the audit found: • there was often limited capacity for early identification of personnel security issues and problems; and • security awareness and education programs could be improved in three of the six organisations audited.

2.71 The effectiveness of the personnel security process is highly dependent on the level of awareness and acceptance of security principles and practices within each organisation. The lack of security awareness is one of the primary risks to an organisation's security, and limits the organisation's ability to protect its classified information. The level of security awareness and culture in three of the six organisations was low, primarily due to a lack of education programs. For example, in three organisations, although staff knew the level of their security clearance, some were unaware of their personnel security responsibilities or the security clearance level required for their position.

2.72 Related to this issue, five of the organisations reviewed did not have effective processes to identify and monitor emerging issues that may be relevant to the ongoing suitability of a clearance subject. Effective personnel security 'aftercare' processes complement the more formal clearance review and reappraisal activity (discussed above). The PSM indicates 'aftercare' processes should be a shared responsibility throughout the whole organisation and not considered to be solely the responsibility of the security section. The audit found three organisations which had controls in place to encourage or support effective personnel security 'aftercare' amongst their line managers and staff but none of the organisations in the audit included an assessment of personnel security awareness in existing performance management programs.

2.73 Finally, three organisations did not have a formal process of security debriefs or exit interviews for staff who leave the organisation. Indeed, in some instances, processes were not in place to ensure the security section was even informed when a security cleared officer left the organisation. Such debriefs reinforce the enduring responsibility to maintain the confidentiality of classified information, and may also highlight potential or emerging security risks.

Conclusion

2.74 Overall, this aspect of personnel security requires significant improvement before meeting the PSM requirements and the principles of effective and efficient management. Areas requiring most attention relate to information management, reconciling and/or integrating the personnel security information with HRMIS addressing outstanding clearance reviews, and improving security awareness programs.

2.75 A lack of effective information management in organisations was reflected at a number of points in the personnel security process. The ability to generate management and other reports from current information is essential to effective management. Indeed, it is one of the contributing factors to the significant problem of clearance review backlogs.

2.76 In terms of gaining assurance about personnel security within the APS the most pressing issue is the reduction of this backlog and the implementation of processes and/or allocation of resources to ensure existing clearances are maintained in accordance with the PSM. An element of this is the integration of personnel security with the general management and creating a strong security culture throughout the organisation.

Recommendation No.7—Information management

2.77 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.

Recommendation No.8—Security clearance reviews

2.78 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.

Implementing the recommendations

2.79 The integration of personnel security information, including the dates of security clearance reviews, would provide the means for more effective management of personnel security information. It would also avoid the need for the maintenance of non-networked records and reduce the attendant risks of error and inconsistency through re-keying information. Additionally, personal security files and other records would be able to be compared and reconciled more effectively with other relevant personnel information.

Recommendation No.9—Security awareness

2.80 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.

Implementing the recommendation

The following strategies to improve personnel security and awareness might be considered:

- including information in the security clearance packs to outline the clearance subject's ongoing responsibilities;
- formal training programs, including e-learning applications, security awareness posters, newsletter articles, log-on screen messages and intranet-based discussion and question/answer pages;
- introducing a regular program of security inspections and security breach reporting, with appropriate recording of actions and any other issues concerning an individual's suitability to hold a security clearance; and
- conveying to all levels of management the message that an effective security regime supports the delivery of business outcomes and is not an added and unnecessary impost.

Recommendation No.10—Security aftercare

2.81 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.

Implementing the recommendation

2.82 Improvements to security clearance aftercare may include, but not be limited to, the following:

- integrating personnel security factors into extant performance management processes. This is an effective and efficient method of continually assessing a clearance subject's suitability and establishing a level of ongoing surveillance between clearance reviews. Additionally, it is an opportunity to encourage reporting of changes in personal circumstance or other matters relevant to personnel security;
- regular promotion of the responsibility of managers and staff to report matters which may impact on security clearances (eg, changes of circumstances, responsibilities and/or suitability); and
- conducting security exit interviews or debriefs for staff with security clearances, particularly for higher level clearances or those considered to be a higher risk, or with access to particularly sensitive information.

Canberra ACT
4 December 2001

P.J. Barrett
Auditor-General

Appendices

Appendix 1

About the audit

Protective Security Audits

PSAs are undertaken as part of the Financial Control and Administration (FCA) audit program introduced by the ANAO in 1995. The program is concerned with improving the quality of public sector administration and aims to assist managers meet their responsibilities by identifying and reporting best practice in areas of financial control and administration. It also provides independent assurance to Parliament about aspects of financial control and administration.

Previous PSA Audit Coverage

Audit Report No.15, 1997–1998, *Internet Security Management*

The objective of this audit was to form an opinion on the effectiveness of Internet security measures within the Commonwealth public sector and to provide better practice guidance for managing an Internet connection. The audit covered a range of Commonwealth organisations which had established an Internet facility. It specifically addressed the following matters:

- Internet security policies;
- site management - including change control processes;
- virus prevention and detection strategies;
- incident response plans;
- controls over access to the Internet site;
- control over data sources connected to the site; and
- user education and training.

Audit Report No.21, 1997–1998, *Protective Security*

The main objectives of the audit were to assess the management and administration of protective security across Commonwealth organisations and to identify, recommend and report better practice in security management. Particular attention was paid to:

- compliance with Government policy, standards and guidelines;
- role of management in protective security; and
- operation of security systems and practices.

The audit criteria and procedures to assess the management and administration of the individual organisations examined were largely based on the overall control framework of an organisation and the guidance provided in the 1991 Commonwealth Protective Security Manual.

Audit Report No.7, 1999–2000, *Operation of the Classification System for Protecting Sensitive Information*

This audit was a follow-on to the 1997–98 Protective Security audit which had found inconsistencies in the identification and marking of classified information, and weaknesses in the management of classified information.

Audit objectives & scope

The objective of this audit was to determine if organisations were managing security clearance and vetting processes effectively and efficiently and in accordance with Commonwealth policy, as shown in the Protective Security Manual (PSM). It was also intended the audit would provide recommendations for improvement (where necessary), and identify and disseminate better practice. In the interests of establishing better practice, organisations were assessed against the revised PSM, despite its recent promulgation.

When planning the audit, the ANAO considered carefully which version of the PSM to utilise as the primary assessment vehicle. Both the 1991 and revised versions of the PSM provide a suitable framework for the development of audit criteria. It was decided the audit would focus on the new PSM as it was more relevant and forward-looking, and the ANAO hoped to assist with its implementation and promote better practices. Other relevant considerations included:

- a draft of the proposed revised PSM was widely circulated to organisations as early as March 1999; and
- there are no significant differences in the personnel security (vetting) standards between the two versions, although the new PSM does contain considerably more informative guidance and discussion.

About the organisations

Seven organisations were selected after appropriate consideration of prior protective security audit coverage, while also addressing the need to achieve a representative sample across the APS. The organisations chosen provided the ANAO with a good mix of both national security and non-national security clearances. Because of the nature of protective security and ANAO's reporting policy for this type of audit, the organisations are not identified in this report.

Audit criteria

For the purpose of the audit, the security clearance process was defined in four stages. These stages are general management; pre-screening and employment; assessment and decision processes; and maintenance, monitoring, and review. The evaluation criteria relevant to each stage are outlined in Table 1 below. Testing at each organisation involved interviews with the ASA or equivalent and other relevant staff, a survey of a sample of security cleared staff and the review of PSFs and other relevant administrative files.

Performance information

Planning for this audit commenced in August 2000 with research into relevant previous reviews and identification of the requirements of PSM. During the planning stage of the audit, the ANAO also consulted with the PSCC and other interested organisations. Broadly, the audit was undertaken in the following stages:

- initial research, planning, and pilot study—August to November 2000;
- in-depth fieldwork—December 2000 to April 2001; and
- reporting—May to November 2001.

The ANAO provided feedback on the results of fieldwork to each organisation included in the audit. This feedback, in the form of a management report, included an assessment of the organisation's performance against each of the evaluation criteria and a set of recommendations relevant to the findings of that organisation. The reports to the organisations included 81 recommendations, 76 (94 per cent) of which were accepted or accepted with qualification.

The duration of the audit, from commencement of planning to the tabling of this report was 16 months and the total cost was $320 000.

Audit evaluation criteria

Table 1 shows the evaluation criteria used for each of the four Audit criteria.

Table 1
Audit evaluation criteria

Audit criteria	*Detailed evaluation criteria*
General management: Policies and procedures Security risk management Position assessments Quality control Training and qualifications	• DSAP/POT assessments reflect the duties and tasks of the position and the organisation's risk profile • Access to classified information without adequate clearance should comply with PSM guidelines • Security Risk Assessments should be current, reflect the current security context and inform the security clearance process • Clearance requirements should reflect the organisation's roles, positions, and classified material holdings • Personnel security policy and procedures have been developed and comply with the PSM • Quality Control processes are in place to ensure early identification of errors or problems • Personnel involved in security clearance and vetting have completed relevant and sufficient training • Cost and efficiency controls are in place and monitored effectively
Pre-screening & employment: Clearance of contractors Eligibility waivers Clearance portability Pre-clearance access	• Contractors require a security clearance appropriate to their access • Eligibility waivers are granted in accordance with PSM guidelines • Organisations recognise clearances from previous organisations and allow portability of clearances • Pre-employment screening should be conducted according to PSM guidelines
Assessment & decision process: Documentation Minimum standards Suitability assessment Decisions and appeals	• Security packages include, at a minimum, the information and forms outlined in the PSM • Subjects are fully informed of the security clearance process and of their rights and obligations • Sufficient and relevant documentation should be retained on the subject's Personal Security File • Background checks and the assessment process complies with PSM in regard to the minimum checks, standards, and principles • Subject and referee interviews are conducted in accordance with the PSM • Assessment of suitability complies with the PSM • Vetting assessment reflects current and relevant risk factors ***continued next page***

Audit criteria	*Detailed evaluation criteria*
	• Understand that ASIO security assessment is not a substitute for security clearance processes • Security clearance decision complies with PSM guidelines • Appeal processes should follow the PSM guidance and reflect the principles of administrative justice
Maintenance, monitoring and review: Clearance reviews Information management Information security Security education and awareness	• Security clearance records administration and management complies with the PSM • Access to the Personal Security File should be strictly controlled • Security clearances are appraised and re-evaluated according to the PSM • Personnel security maintenance and awareness is integrated into day to day organisation management

Appendix 2

Overview of Commonwealth Protective Security Manual 2000

The new PSM comprises eight parts, the purpose of each part is briefly outlined below.

Part A **Protective Security Policy**
To provide clear direction on the standards expected by the Commonwealth with regard to the securing of its resources and the safeguarding of its functions.

Part B **Guidelines on Managing Security Risk**
To provide a detailed framework for developing and implementing a security risk management plan appropriate to the organisation's functions.

Part C **Information Security**
To provide guidance on the classification system and the protective standards required to protect security classified information - both electronic and paper-based.

Part D **Personnel Security**
To provide a set of standards and procedures in relation to personnel security practices.

Part E **Physical Security**
To provide advice on creating physical environments appropriate for the protection of Government resources and the provision of Government services to the public.

Part F **Security Framework for Competitive Tendering and Contracting (CTC)**
To provide organisation management with a comprehensive outline of their responsibilities in relation to security when outsourcing specific organisation functions. This part also provides guidance to ensure that appropriate security precautions are undertaken by contractors and their employees when handling official information / performing government functions.

Part G **Guidelines on Security Incidents and Investigations**
To assist organisations in the conduct of investigation of security breaches and incidents. This part provides detailed information regarding employees' obligations under the Contact Reporting Scheme.

Part H **Security Guidelines on Home-based Work**
To provide information, standards and procedures on security where Commonwealth employees seek to work from home.

Index

Series Titles

Titles published during the financial year 2001–02

Audit Report No.21 Performance Audit
Developing Policy Advice
Department of Education, Training and Youth Affairs, Department of Employment, Workplace Relations and Small Business, Department of Family and Community Services

Audit Report No.20 Performance Audit
Fraud Control Arrangements in the Department of Agriculture, Fisheries and Forestry—Australia (AFFA)
Department of Agriculture, Fisheries and Forestry—Australia

Audit Report No.19 Assurance and Control Assessment Audit
Payroll Management

Audit Report No.18 Performance Audit
Performance Information in Portfolio Budget Statements

Audit Report No.17 Performance Audit
Administration of Petroleum Excise Collections
Australian Taxation Office

Audit Report No.16 Performance Audit
Defence Reform Program Management and Outcomes
Department of Defence

Audit Report No.15 Performance Audit
Agencies' Oversight of Works Australia Client Advances

Audit Report No.14 Performance Audit
Client Service Initiatives Follow-up Audit
Australian Trade Commission (Austrade)

Audit Report No.13 Performance Audit
Internet Security within Commonwealth Government Agencies

Audit Report No.12 Financial Control and Administration Audit
Selection, Implementation and Management of Financial Management Information Systems in Commonwealth Agencies

Audit Report No.11 Performance Audit
Administration of the Federation Fund Programme

Audit Report No.10 Assurance and Control Assessment Audit
Management of Bank Accounts by Agencies

Audit Report No.9 Performance Audit
Learning for Skills and Knowledge—Customer Service Officers
Centrelink

Audit Report No.8 Assurance and Control Assessment Audit
Disposal of Infrastructure, Plant and Equipment

Audit Report No.7 Audit Activity Report
Audit Activity Report: January to June 2001
Summary of Outcomes

Audit Report No.6 Performance Audit
Commonwealth Fisheries Management: Follow-up Audit
Australian Fisheries Management Authority

Audit Report No.5 Performance Audit
Parliamentarians' Entitlements: 1999–2000

Audit Report No.4 Performance Audit
Commonwealth Estate Property Sales
Department of Finance and Administration

Audit Report No.3 Performance Audit
The Australian Taxation Office's Administration of Taxation Rulings
Australian Taxation Office

Audit Report No.2 Performance Audit
Examination of Allegations Relating to Sales Tax Fraud
Australian Taxation Office

Audit Report No.1 Financial Statement Audit
Control Structures as part of the Audits of the Financial Statements of Major Commonwealth Entities for the Year Ended 30 June 2001

Better Practice Guides

Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	Jun 2001
Internet Delivery Decisions	Apr 2001
Planning for the Workforce of the Future	Mar 2001
Contract Management	Feb 2001
AMODEL Illustrative Financial Statements 2001	May 2001
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Managing APS Staff Reductions (in Audit Report No.47 1998–99)	Jun 1999
Commonwealth Agency Energy Management	Jun 1999
Corporate Governance in Commonwealth Authorities and Companies–Principles and Better Practices	Jun 1999
Managing Parliamentary Workflow	Jun 1999
Cash Management	Mar 1999
Management of Occupational Stress in Commonwealth Agencies	Dec 1998
Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	Oct 1998
New Directions in Internal Audit	Jul 1998
Life-cycle Costing (in Audit Report No.43 1997–98)	May 1998
Controlling Performance and Outcomes	Dec 1997
Management of Accounts Receivable	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997
Public Sector Travel	Dec 1997
Audit Committees	Jul 1997
Core Public Sector Corporate Governance (includes Applying Principles and Practice of Corporate Governance in Budget Funded Agencies)	Jun 1997
Administration of Grants	May 1997

Management of Corporate Sponsorship	Apr 1997
Telephone Call Centres	Dec 1996
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Performance Information Principles	Nov 1996
Asset Management	Jun 1996
Asset Management Handbook	Jun 1996
Managing APS Staff Reductions	Jun 1996