The Auditor-General
Audit Report No.43 2006–07
Performance Audit

Managing Security Issues in Procurement and Contracting

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 80963 1

Australian National Audit Office

Canberra ACT
13 June 2007

Dear Mr President
Dear Mr Speaker

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

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

Ian McPhee
Auditor-General

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

AUDITING FOR AUSTRALIA

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

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

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

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

http://www.anao.gov.au

Audit Team

Bill Bonney
Harit Wadhawan
Andrew Morris

Contents

Abbreviations

ANAO	Australian National Audit Office
ACSI 33	Australian Government Information and Communications Technology Security Manual
CPGs	Commonwealth Procurement Guidelines
ComSuper	Commonwealth Superannuation Administration
Customs	Australian Customs Service
DFAT	Department of Foreign Affairs and Trade
Finance	Department of Finance and Administration
ICT	Information and Communications Technology
PSM	Protective Security Manual
RFT	Request for Tender

Glossary

Approach to the market	A notice or request that invites prospective contractors to submit proposals for the performance of specified services or the supply of specified goods.
Conditions for participation	Mandatory requirements or standards to be met before a prospective contractors' submission or proposal can be considered for a planned procurement.
Contract	A legally enforceable agreement between two parties, which contains, amongst other things, terms and conditions relevant to the agreement, rights and obligations or responsibilities of each party and the agreed outcomes of the relationship.
Contractor	A person or business entity that has entered into a contract with an Australian Government agency for the performance of services for, or supply of goods to, that agency.
Evaluation criteria	The factors or requirements that eligible submissions from prospective contractors are assessed against.
Protective security	Policies, principles, standards and procedures to be followed by all Australian Government agencies in the protection of official resources.
Security clearance	The process of assessing a person's eligibility and suitability for access to security classified information through a comprehensive evaluation of their history, attitudes, values and behaviour.
Security classified information	Official information that must be afforded a level of protection to safeguard it from compromise or unauthorised use because it could cause harm, or have adverse consequences.

Security incident	A security event, including an accidental failure to observe security requirements, a reckless or deliberate act, or an unauthorised attempt to obtain official information that leads, or could lead to, the loss, damage or compromise of official information.
Security risk	An event that could result in the compromise of official resources. Security risks are measured in terms of their probability and consequences.
Third party interest	Any legal right, interest or power in favour of any person in connection with the parties to a contract, including any right of access, repossession, receivership, control, or other interest.

Summary and Recommendations

Summary

Background

1. Australian Government agencies have a responsibility to protect the resources they manage on behalf of all Australians. These resources are considerable. For example, in 2005–06 the general government sector[1] held assets worth $206 billion.[2] Australian Government agencies also generate and hold extensive information relating to their activities, which they need to safeguard for privacy, commercial, and other reasons.

2. Protective security describes the policies and practices used by an agency to protect its resources, including the official information it generates and receives. A sound protective security environment is an important element in the management of an agency's human, information and physical resources.[3] The Protective Security Manual (PSM) is the main source of protective security policies, principles and responsibilities for Australian Government agencies. The PSM provides guidance on the policies and practices important in the development of an effective protective security function. It also prescribes the minimum protective security standards for Australian Government agencies to maintain.

3. Contracting is an integral part of the way Australian Government agencies conduct business. In 2005–06, Australian Government agencies entered into around 48 000 contracts worth $14.8 billion to provide a variety of business and administrative services across the range of activities.[4] Given the large number of contractors providing services to Australian Government agencies, and the extensiveness of their access to these agencies' assets and information, it is important that agencies manage security risks associated with the use of contractors.

4. When engaging in procurement and contracting activities, Australian Government agencies must act in accordance with the policy framework

---

1 The general government sector comprises those Australian Government departments and agencies that provide non-market public services. They are predominantly funded through Parliamentary appropriations.

2 Commonwealth of Australia, *Consolidated Financial Statements for the year ended 30 June 2006*, December 2006, p. 76.

3 Attorney-General's Department, *Protective Security Manual 2005*, Commonwealth of Australia, p. A3.

4 Extracted from *AusTender—Contracts Reported*. Viewed at <www.contracts.gov.au> on 17 April 2006.

contained in the Commonwealth Procurement Guidelines (CPGs). Additionally, they must adhere to the legislative requirements and standards encompassed in a range of Australian Government general policies.[5] Protective security is one of these general policies, and the PSM is the source of further guidance. The PSM specifies, in Part F, that Australian Government agencies are responsible for managing security issues and risks, including the risk of unauthorised access to, or the loss of, security classified information, involved in the use of contractors.

5. For the purposes of this audit, procurement refers to agencies' efforts to arrange for the purchase of services, up to and including the point of signing a contract. Contracting refers to the delivery of these services by the provider, subsequent to their appointment. As such:

- procurement incorporates: planning the purchase; approaching the market; evaluating tender responses; and executing the contract (including establishing security requirements in the contract); and
- contracting incorporates: providing security training to contractors; managing the contractors' performance, including their adherence to relevant security requirements; and the mechanisms used to identify, report and record the details of any security breaches by contractors.

Audit approach

6. The objective of this audit was to evaluate whether selected Australian Government agencies were effectively managing security risks arising from the use of contractors. To address this objective, the audit evaluated relevant policies and practices in the audited agencies against a series of minimum requirements in the management of security issues in procurement and contracting activity. These minimum requirements were developed from the guidance and standards contained in the PSM and also from the ANAO's previous protective security audits.

[5] Department of Finance and Administration, *Financial Management Guidance No.10—Guidance on Complying with Legislation and Government Policy in Procurement*, January 2005, p. 5.

7. The audit focused on two broad types of contracting arrangements: contracting of security functions; and contracting of any service or business function that requires, or which has the potential to require, contractors to access sensitive or security classified information.

8. The following Australian Government agencies were involved in this audit:

- Australian Customs Service (Customs);
- Commonwealth Superannuation Administration (ComSuper);
- Department of Finance and Administration (Finance); and
- Department of Foreign Affairs and Trade (DFAT).

9. In addition, the Attorney-General's Department, which is responsible for the maintenance of the PSM and for providing advice on contemporary protective security policies and practices, was consulted during the audit.

Audit conclusion

10. Overall, the ANAO concluded that the audited agencies were effectively managing security risks during the procurement phase when contracting-out security functions or functions that may require contractors to access sensitive information. However, the audit identified scope to improve the management of security risks once contractors had been appointed.

11. While the audited agencies typically could have improved guidance to staff about addressing security risks in procurement, the agencies, nevertheless, generally adequately considered security risks when: planning procurements; approaching the market; executing contracts; and, to a lesser extent, evaluating tenders.

12. The audited agencies generally provided adequate security awareness training programmes for new contractors. Overall, however, they could have improved processes and practices to: ensure that appointed contractors attended security training; monitor contractors' adherence to security requirements in contracts; and reassess security risks in contracts when circumstances changed substantially, or when contracts were extended significantly beyond their original life.

13. The ANAO found that at the four audited agencies, there was a record of only one recent security breach involving a contract examined during the audit. While this suggests that contractors may have largely adhered to

security requirements, the ANAO notes that security breaches are sometimes not reported. In this regard, one of the audited agencies did not have a system to effectively monitor and report such incidents.

14. There was considerable variation between the agencies in the extent to which they adhered to the minimum requirements for the management of security risks in procurement and contracting examined as part of this audit. The ANAO assessed one of the agencies as meeting virtually all of these requirements, two agencies as meeting most of these requirements, but the remaining agency as meeting few of these minimum requirements.

15. Amongst the audited agencies, the ANAO identified several practices that it considered to be good examples of managing security risks and issues involved in procurement and contracting activity. These practices are shown in Table 1.

Table 1

Better practices to manage security risks in procurement and contracting activity

Component of procurement and contracting activity	Better practice
Procurement planning	One agency included a reference to its security policy on managing security risks in procurement activity in its procurement and contracting policy material. One agency included guidance notes in its model *Request for Tender* template to assist staff develop the security requirements and obligations to be imposed on prospective contractors.
Orientation and training	One agency required staff and contractors to acknowledge, in writing, their security responsibilities every year. Two agencies had induction activities in individual work-areas to supplement agency-wide security awareness training programmes. Two agencies required all staff and contractors to attend security awareness refresher training. One agency included details of attendance at security awareness training in reports to its executive.
Managing contracts	At two agencies, contractors were required (and did) submit regular reports on progress or performance against security-related obligations.

Source: ANAO.

Key findings

Managing security issues in procurement

Policies and guidance material

16. Each of the audited agencies had promulgated a number of detailed procurement and contract-related policies and guidance material. In each case, this information included references to applicable legislation, regulations, and other relevant aspects of the Australian Government procurement policy framework (such as the CPGs). Generally, however, these procurement and contract-related policy documents contained only a limited amount of information on managing security issues and risks.

17. Three of the audited agencies did, however, include information on managing security issues and risks involved with procurement and contracting activities in their security policies. Of these, the ANAO considered that only one agency had properly addressed the scope of the PSM regarding the management of security issues in procurement and contracting activity.

Model tender and contract templates

18. Each of the audited agencies had developed model *Request for Tender* and contract templates and had made these available to staff involved in the engagement of contractors.

19. Three of the audited agencies' tendering templates contained details of, and obliged respondents to adhere to, applicable security requirements. For the most part, the audited agencies' model contract templates designed for use in the more-complex and higher-risk procurements contained clauses consistent with most of the requirements of the PSM (*Part F—Security Framework for Procurement)*.

Procurement planning

20. At three of the audited agencies, nearly all of the procurement planning documentation examined contained an assessment of security issues relevant to the proposed procurement. In most cases, the assessments related to whether the contractor(s) would, or may, require access to security classified information, and also considered the attendant security clearance requirements. At the remaining agency, while procurement planning documentation considered a range of pertinent business risks, it did not specifically identify, or assess, security risks.

Approaching the market

21. Across the audited agencies, most of the *Request for Tender* or equivalent documentation examined during the audit contained references to the security requirements relevant to the proposed engagement. Typically, this documentation included a reference to the agency's security policies or instructions, and highlighted that the contractor would, or may, require access to security classified information and therefore would require a security clearance.

Evaluating tenders

22. The ANAO found that tender evaluation processes had properly considered the security requirements contained in documentation provided to the market in all but two of the 30 contracts examined in this part of the audit. In the two contrasting cases, the agencies relied solely on assurances from prospective contractors that security requirements had been met. The ANAO considered, in both of these cases that the agencies should have confirmed through review, or otherwise obtained positive assurance at the time of evaluation, that the security requirements had been properly met.

23. At three of the audited agencies the ANAO found that a member of the agency's protective security team had been involved, or consulted, in many of the tender evaluation processes examined. In the other cases examined at these agencies, the ANAO considered the staff involved in the evaluation process demonstrated a good understanding of the pertinent security issues and requirements. At the fourth agency, there was no evidence that tender evaluation processes had involved a person(s) with knowledge of protective security issues or standards.

Content of contracts

24. Overall, most of the contracts examined addressed most of the relevant requirements contained in the PSM. For example, all but one of the contracts reviewed were found to contain details of the security requirements relevant to the services being contracted-out. In addition, most of the contracts examined also stated that these security requirements could be amended during the life of the contact.

25. Despite the reasonably comprehensive coverage of security requirements in most of the contracts examined, around half of the contracts examined did not:

- contain a clause(s) dealing with the risk of access to the agency's information through a third party interest; and
- explicitly identify a breach of security requirements as a reason to terminate the contract.

26. One of the reasons why many contracts examined did not contain these two clauses is likely to be that most of the audited agencies' model contract templates did not contain these clauses.

Managing security issues in contracting

Orientation and training

27. At three of the audited agencies, contractors were required to attend the agency's formal security awareness training for 'new starters'. However, one agency had only made it mandatory for new contractors to attend security awareness training in late-2006. At the remaining agency, although contractors were not required to attend security awareness training provided to 'new starters', the agency advised the ANAO that they may have been provided a security briefing at the time they commenced work.

28. Overall, the ANAO found that the audited agencies were delivering security awareness training programmes that addressed most of the key security issues. For example, the training at each agency: explained the reasons why security awareness was important; promoted an understanding of the agency's security policies; and provided clarity on attendant roles and responsibilities.

29. At the time of the audit, each of the audited agencies had a range of processes for identifying those staff and contractors required to attend security awareness training. Each of the audited agencies also maintained records of those staff and contractors attending security awareness training. However, testing of attendance records has suggested that a significant number of contractors engaged under the contracts being examined may not have attended security awareness training.

Contract management

30. In three of the audited agencies, nearly all the contracts reviewed contained a clause(s) relating to the management of the contractor's performance. In the remaining agency, only four of the 13 contracts reviewed contained such a clause(s).

31. For the most part, contract management provisions in the contracts examined related to the provision of reports on, and the conduct of regular meetings about, the services being provided. Specifically, in relation to the management of security issues and requirements, the ANAO found that:

- several contracts at one agency listed penalties (other than terminating the contract) for the failure to meet security requirements;
- at one agency, all of the contracts provided that contractors must submit security reports and participate in security reviews, when requested to do so;
- several of the contracts examined at two agencies required the contractors to submit regular reports on security progress or performance; and
- six of the contracts examined at another agency required contractors to participate, at least annually, in reviews of the operation of security requirements.

32. Across the four audited agencies, the ANAO observed a variety of mechanisms to manage the performance of contractors. This included holding regular meetings, reviewing status reports, inspecting work and, in a few cases, monitoring results against service standards or key performance indicators. However, the use of such systematic mechanisms was not common or consistent.

33. The ANAO found, in only seven of the 43 contracts examined in this part of the audit, that agencies were systematically assessing security performance or measuring compliance with security requirements. Generally, the audited agencies indicated that security matters were only considered if, and when, matters arose. Some of the contract managers interviewed suggested they relied on the agency's broader security programs and policies to provide them assurance that security requirements were being complied with.

Review of security risks/requirements

34. While each of the audited agencies required risk assessments to be undertaken to support spending proposals related to contract extensions, none specifically addressed, in relevant policy documents, the need to consider security issues during such assessments. In addition, none of the agencies had policies requiring security risks to be reviewed when there has been a change in a contract's circumstances that is likely to affect these risks.

35. Fourteen of the contracts examined had either been extended beyond their original term, or the services being provided had been affected by a significant change in circumstances. The ANAO found, in only half of these cases, that the decision to extend or continue the contractual arrangement was supported by a re-assessment of the security risks and requirements involved.

Security incidents

36. Most of the contracts reviewed during the audit contained a clause(s) requiring the contractor to advise the agency of any security incidents. Three of the audited agencies had agency-wide processes for identifying, reporting, recording and monitoring breaches of security and other security incidents. The fourth agency did not have a system for effectively capturing details of security incidents.

Agencies' comments

37. Each of the audited agencies, together with the Attorney-General's Department, agreed with the recommendations in this report. The agencies' responses to each of the recommendations are shown in the body of the report. Where provided, agencies' general comments are shown at Appendix 2.

Recommendations

The following recommendations are based on the findings of the fieldwork at the audited agencies. The ANAO considers that these recommendations are relevant to all Australian Government agencies. Therefore, all Australian Government agencies should assess the benefits of implementing the recommendations in light of their own circumstances, including the extent that each recommendation, or part thereof, is addressed by practices already in place.

Recommendation No. 1

Paragraph 2.27

To assist staff to manage security risks during procurement and contracting activities, the ANAO recommends that Australian Government agencies:

(a) include in protective security and procurement/contracting policy documents, information on the security risks of using contractors that is appropriate for their operations; and

(b) update model procurement and contract templates to fully reflect the requirements of the PSM (*Part F—Security Framework for Procurement*).

Recommendation No. 2

Paragraph 3.29

As part of ongoing contract management, the ANAO recommends that Australian Government agencies adopt a risk-based approach to monitoring and evaluating the performance of contractors, including their adherence to security requirements. This approach should require agencies to re-evaluate security risks of contracts that are affected by a significant change in circumstances, or which are extended significantly beyond their original term.

Agencies' responses to the recommendations

38. Each of the audited agencies, together with the Attorney-General's Department, agreed to the recommendations. The agencies' responses to each recommendation are shown in the body of the report.

Audit Findings and Conclusions

1. Introduction

This chapter provides background information about the audit, including an overview of protective security requirements for contractors, and details of the audit approach.

Protective security

1.1 Australian Government agencies have a responsibility to protect the resources they manage on behalf of the Australian population. These resources are considerable. For example, in 2005–06, the general government sector[6] held assets worth $206 billion, including $93 billion in cash and investments, $41 billion relating to items of plant and equipment, and $21 billion worth of land and buildings.[7] Australian Government agencies also generate and hold extensive information relating to their activities, which they need to safeguard for privacy, safety, good governance, commercial and in some cases, national security reasons.

1.2 Protective security describes the policies and practices used by an agency to protect its human, information and physical resources.[8] An effective protective security environment encompasses a range of complementary measures across the following dimensions:

- physical security: comprising equipment and other measures designed to prevent and detect unauthorised access to official information and resources; such as closed circuit television systems, alarms, secure containers and access-control devices or barriers;
- information security: comprising procedures designed to protect official information from compromise, loss, corruption or unauthorised disclosure. These measures include the classification of information, applying protective markings and adopting special handling measures for the use, storage, transmission and disposal of information;

6 The general government sector comprises those Australian Government departments and agencies that provide non-market public services. They are predominantly funded through Parliamentary appropriations.

7 Commonwealth of Australia, *Consolidated Financial Statements for the year ended 30 June 2006*, December 2006, p. 76.

8 Attorney-General's Department, *Protective Security Manual 2005*, Commonwealth of Australia, p. A3.

- personnel security: the conduct and ongoing maintenance of security clearances for those people requiring access to security classified information. Other essential aspects of personnel security are the maintenance of security awareness levels and upholding the 'need to know' principle;
- information and communications technology security: comprising activities designed to protect the integrity of information and communications technology systems and the information they contain or transmit. Critical controls include system certification and accreditation, logical access restrictions, audit trails, storage protocols, data encryption, authenticating transmissions and connectivity standards; and
- security incidents and investigations: comprising procedures to identify, report, record and, as appropriate, investigate incidents involving a failure to observe security requirements, or of actions or behaviour that could lead to the loss, damage, corruption or unauthorised disclosure of official resources.

1.3 These elements need to be subject to robust oversight and coordination to help ensure they are delivered in a consistent and complementary manner. This is often best achieved when protective security is managed together with other critical functions, such as risk management, to form a key element of each agency's governance framework.

1.4 The Protective Security Manual (PSM) is the main source of protective security policies, principles and responsibilities for Australian Government agencies.[9] The PSM provides guidance and advice on the policies and practices important in the development of an effective protective security function. It also prescribes the minimum protective security standards for Australian Government agencies to maintain.

[9] The latest version of the PSM was released by the Attorney-General in August 2005, replacing the October 2000 edition. Unless otherwise indicated, references to the PSM in this report refer to the new version. In the few instances where this report refers to the previous PSM, it draws on descriptions contained in that document of ways agencies can satisfy certain security requirements.

Protective security requirements for procurement and contracting

1.5 Procurement and contracting is an integral part of the way Australian Government agencies conduct business.[10] In 2005–06, Australian Government agencies entered into around 48 000 contracts worth $14.8 billion, to provide a variety of business and administrative services across the range of responsibilities.[11]

1.6 For the purposes of this audit, procurement refers to agencies' efforts to arrange for the purchase of goods and services, up to and including the point of signing a contract. Contracting refers to the delivery of goods and services by the provider, subsequent to their appointment. As such:

- procurement incorporates: planning the purchase of goods and services; approaching the market; evaluating tender responses; and executing contracts (including establishing security requirements contained in the contract); and
- contracting incorporates: providing security training to contractors; managing the contractors' performance, including their adherence to relevant security requirements; and the mechanisms used to identify, report and record the details of any security breaches by contractors.

1.7 Given the large number of contractors providing business and administrative services to the Australian Government agencies at any point in time, and the extensiveness of their access to Australian Government assets and information, it is important that agencies manage security risks associated with the use of contractors.

1.8 When engaging in procurement and contracting activities, Australian Government agencies must act in accordance with the policy framework contained in the Commonwealth Procurement Guidelines (CPGs). Additionally, they must adhere to the legislative requirements and standards encompassed in a range of Australian Government general policies. *Financial Management Guidance No.10—Guidance on Complying with Legislation and Government Policy in Procurement*[12] lists the general policies that are relevant to

---

[10] ANAO *Better Practice Guide: Developing and Managing Contracts—Getting the Right Outcome, Paying the Right Price*, February 2007, p. 2.

[11] Extracted from *AusTender—Contracts Reported*. Viewed at <www.contracts.gov.au> on 17 April 2006.

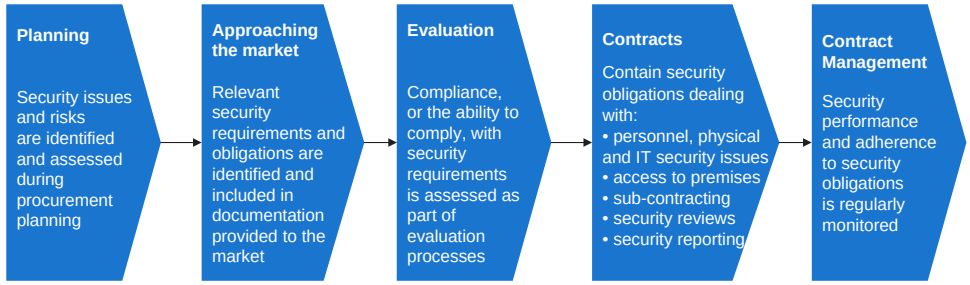
[12] Department of Finance and Administration, *Financial Management Guidance No.10—Guidance on Complying with Legislation and Government Policy in Procurement*, January 2005, Part 4.

procurement activity. It also identifies, for each policy, the attendant legislation or authority. It identifies protective security amongst the general policies, and lists the PSM as the source of further guidance.

1.9 Part F of the PSM, *Security Framework for Procurement,* discusses the principles involved, and outlines the standards to be met, to minimise the risks to official Australian Government resources during procurement and contracting activity. In particular, the PSM states that outsourcing a function does not relinquish Australian Government agencies from their responsibility or accountability for the effective performance of that function. The PSM requires security issues to be considered and managed throughout the key stages of procurement and contracting activity. Figure 1.1 illustrates the main components of managing security issues during procurement and contracting activity covered in the PSM.

Figure 1.1

Managing security issues during procurement and contracting activities



Source: ANAO, based on the PSM (Part F).

Audit approach

Background to protective security audits

1.10 Following a recommendation from the 1979 *Inquiry into Protective Security*, undertaken by Mr Justice Hope, the Australian National Audit Office (ANAO) commenced a program of audits to evaluate protective security arrangements in Australian Government agencies. In the majority of cases, these audits were conducted and reported on an individual organisation basis (that is, independently from each other). In 1995, the ANAO included protective security audits in its cross-agency general performance audit programme, which is undertaken pursuant to section 18 of the *Auditor-General*

Act 1997. This section provides that the ANAO may examine a particular aspect of the operations of the whole, or of a part of the Australian Government sector.

1.11 This is the eighth cross-agency protective security audit conducted by the ANAO under these arrangements. Appendix 2 lists the earlier protective security audits undertaken by the ANAO.

Audit objectives and criteria

1.12 The objective of this audit was to assess whether selected Australian Government agencies were effectively managing the security risks arising from the use of contractors. To address this objective, the audit evaluated the policies and practices at each of the audited agencies against a series of minimum requirements relating to the management of security issues in procurement and contracting activity. These minimum requirements were developed from the guidance and standards contained in the PSM and also from the ANAO's previous protective security audits.

1.13 Table 1.1 shows these requirements, grouped into four components.

Table 1.1

Minimum requirements in managing security issues during procurement and contracting activities

Component	Minimum requirement
Procurement planning and approaching the market	Policy and guidance documents, including model tendering and contract templates, are available to inform and assist staff to deal with the security risks and requirements involved in contracting-out functions. The security risks and requirements associated with the contracted function are identified and assessed as part of procurement planning. The security requirements or obligations associated with the contracted function, including relevant minimum standards in the PSM, are included in the approach to the market.
Evaluating tenders	The contractor's ability to meet the security requirements relevant to the engagement has been evaluated.
Orientation/training	Contractors are provided with agency-specific protective security awareness training, including advice about the agency's security-related policies and procedures.
Managing the contractor's security-related performance	Contracts detail the security requirements associated with the contracted-out function and meet other minimum requirements contained in the PSM. Regular assessments are undertaken as to whether contractors have adhered to the security requirements and related obligations contained in the contract. The agency monitors security risks and associated requirements during the life of each contract, particularly if there have been any changes in contractual arrangements.

Source: ANAO, based mainly on the PSM.

Audit scope

1.14 The audit focused on two broad types of contracting arrangements:

- contracting of protective security services or functions: for example; guarding services; the conduct of security clearances; the maintenance of security equipment; or the conduct of security investigations; and
- contracting of any service or business function that requires, or which has the potential to require, contractors to access sensitive or security classified information: for example; engaging information and communications technology contractors; records management; payroll processing; or property management services such as cleaning, or the disposal of classified waste.

Audit coverage

1.15 The following Australian Government agencies were involved in this audit:

- Australian Customs Service (Customs);
- Commonwealth Superannuation Administration (ComSuper);
- Department of Finance and Administration (Finance); and
- Department of Foreign Affairs and Trade (DFAT).

1.16 At each of these agencies, fieldwork involved a series of interviews with key staff, a review of relevant policy and associated guidance documentation, and the examination of files and other records relating to a sample of contracts entered into by the agency. Following the conduct of audit fieldwork, each of the audited agencies was provided with a management report detailing the audit findings, conclusions and, where appropriate, recommendations for improvement specific to them.

1.17 Across the four audited agencies, the ANAO examined a total of 44 contracts. Contracts were selected for examination based on their value and the nature of the service provided. In particular, as mentioned at paragraph 1.14, the audit focussed on contracts involving security functions, or contracts that required, or potentially required, contractors to access sensitive or security classified information. A break-down of the nature of the contracted services examined during the audit is shown in Table 1.2.

Table 1.2

Nature of contracted services examined in the audit

Nature of contracted services	Number of contracts tested
A protective security-related function, including IT security	16(1)
Property management	5
Records or information management	3
Other IT-related services	18
Payroll-related	2
Total	**44**

Notes: (1) One of the contracts selected for examination was still being finalised and had not been signed at the time of the audit. Accordingly, it was only evaluated against the following requirements in Chapter 2: procurement planning; approaching the market; and evaluating tenders.

Source: ANAO, based on testing.

1.18 The Attorney-General's Department, which is responsible for the maintenance of the PSM and for providing advice on contemporary protective security policies and practices, was consulted during the audit.

1.19 The audit engaged Courage Partners Pty Ltd to assist with the conduct of audit fieldwork and the production of management reports at two of the audited agencies. The audit was conducted in accordance with the ANAO's Auditing Standards and was completed at a cost of approximately $270 000.

Audit reporting and structure

1.20 The audit recommendations in protective security audit reports are framed to have general application and the audit findings are reported to Parliament in generic terms, without being attributed to particular agencies. Where appropriate, this report also includes references to sound and better practices identified during the audit.

1.21 The results of the audit, together with recommendations for improving the management of security issues involved in procurement and contracting activity, are set out in Chapters 2 and 3. Chapter 2 deals with the management of security issues relating to the procurement phase: procurement planning; approaching the market; evaluating tenders; and executing contracts. Chapter 3 deals with the management of security issues after the commencement of each contract: orientation and training of contractors; managing performance, including adherence to relevant security requirements; and the mechanisms used to identify and record details of any security breaches.

1.22 Comments provided by each of the audited agencies, together with the Attorney-General's Department are shown in Appendix 1. As mentioned earlier, Appendix 2 lists the protective security audits previously undertaken by the ANAO.

2. Managing Security Issues in Procurement

This chapter discusses audit findings and better practices identified in the agencies audited relating to managing security issues during the procurement phase. It examines procurement planning, approaching the market, evaluating tenders, and the inclusion of security requirements in contracts.

Procurement planning and approaching the market

2.1 To effectively manage security risks when contracting-out security functions or functions that may require contractors to access sensitive information, it is important that agencies consider security requirements during the procurement planning phase.

2.2 The extent to which agencies consider security matters during procurement planning will depend on the risks involved in the proposed procurement. Factors impacting on the level of security risk include whether contractor(s) may:

- be required to access any classified or sensitive information;
- be working at the agency's, or their own, premises or at another external location; and
- require access to the agency's information and communications technology systems, including through remote access facilities.

2.3 To assess the adequacy of the management of security-related issues during procurement planning and the approach to the market, the ANAO considered:

- whether the audited agencies developed and promulgated sufficient policy and guidance material, including well-designed model tendering and contract templates, to assist security-related decision-making during procurement activity; and

- for each of the selected contracts, whether:
  - procurement planning included the identification and assessment of security-related risks associated with the proposed contractual arrangements;[13] and
  - the approach to the market contained details of relevant security requirements and, where necessary, referred to the minimum standards in the PSM covering the handling of security classified information.[14]

Policy and guidance material

2.4 To assist staff manage security risks involved in procurement and contracting, agencies should have appropriate and up-to-date policy and guidance material. A lack of suitable policy and guidance material can lead to inconsistencies and misunderstandings in relation to the issues and risks involved, resulting in poor decision-making.

2.5 The nature and content of policy and guidance material relating to the management of security risks in procurement and contracting should reflect: the nature of the agency's work and information holdings; the security risks it is exposed to; and the nature and significance of relevant security incidents that have occurred. At a minimum, the ANAO expected that policy and guidance material dealing with the management of security risks in procurement and contracting should contain a reference to the minimum standards in the PSM (Part F). In addition the ANAO considers that agencies' policy and guidance material should assist officers to:

- assess security-risks during procurement planning;
- consider the security issues involved with the proposed contractual arrangements when developing the Request for Tender (RFT), including, for example, whether contractors may be required to access security classified information or hold security-related accreditations;
- develop tender evaluation plans, which reflect, and provide for, due consideration to be given to relevant security requirements;
- incorporate clauses in contracts that require contractors to adhere to security requirements, including the agency's specific security policies,

[13] As required under Part F of the PSM, paragraph 2.4.

[14] As required under Part F of the PSM, paragraphs 2.5 and 4.4.

and provide for the termination of the contract for a failure to meet security requirements; and

- establish robust contract management arrangements, including setting-up security-related reporting, auditing and review mechanisms.

2.6 This information should be contained in one, if not both, of the agencies' procurement/contracting, and protective security policy documents. At the very least, however, these policy documents should be consistent, be cross-referenced to each other, and together provide guidance on the information outlined above.

Procurement and contracting policy and guidance material

2.7 When agency staff commence procurement activities, an initial step typically is to examine procurement and contracting policies and guidance material. It is therefore important that this guidance material addresses the management of security risks in contracting, either directly or with reference to the agency's security policy and guidance material.

2.8 Reflecting the importance of procurement and contracting activity to their operations, each of the audited agencies had promulgated a number of detailed procurement and contract-related policies and guidance material. In each case, this information included references to applicable legislation, regulations, and other relevant aspects of the Australian Government procurement policy framework (such as the CPGs).

2.9 Generally, however, the procurement and contract-related policy documents reviewed during the audit contained only a limited amount of information on managing security issues and risks. Only two of the audited agencies highlighted, in their procurement and contract-related policy documents, information on the need to manage security risks when involved in procurement and contracting activity. Further, only one agency included a reference to its relevant security policy document in its procurement and contract-related policies.

Security policy and guidance material

2.10 Security policy and guidance material inform staff about the policies and practices employed by an agency to address security risks associated with its operations and functions. In most agencies, this should include information on managing security risks involved in procurement and contracting activity.

2.11 The ANAO found that three of the audited agencies included information on the management of security issues and risks in procurement and contracting activities in their security policies. The fourth agency, however, did not include any relevant information or guidance material in its security policies. Nor did this agency have any such guidance material in its procurement/contracting policies.

2.12 Overall, however, the ANAO considered that only one of the audited agencies had security policy documents containing information on managing security issues in procurement and contracting activity that fully addressed the scope of the PSM (Part F).

2.13 Of the two other agencies that included information on the management of security issues and risks in procurement and contracting activities in their security policies:

- one agency's security policy documentation highlighted the need to manage security risks during procurement activity and also contained a reference to the PSM (Part F). However, it did not contain any discussion on, nor did it illustrate, the security issues and risks involved in the use of contractors; while
- the other agency's relevant security policy document did not address four major aspects of procurement and contracting covered in the PSM: procurement planning; approaching the market; evaluation processes; and contract management.

Model tender and contract documentation

2.14 A common way to assist staff involved in procurement activities is to promulgate model tendering and contracting templates. These templates should be aligned to relevant guidance material. These model templates can cover a range of issues, such as managing the security risks in contracts, even if broader guidance does not.

2.15 The ANAO found that each of the audited agencies had developed a range of model RFT and contract templates and made them available to staff involved in the engagement of contractors. At one agency, the ANAO was advised that individual business-lines also maintained procurement-related templates designed to meet their own procurement requirements.

2.16 Each of the agencies had a specialised section or team responsible for assisting line areas during the procurement process, including, where relevant, providing advice on the most relevant template to use. These sections were

also responsible for reviewing the reasonableness of draft tenders and contracts in light of the risks, complexity and value of proposed procurements. Amongst other things, these reviews assessed whether the agency's security requirements had been addressed, and considered whether additional security requirements may be required.[15]

2.17 The ANAO also assessed whether the model tender and contract templates at the audited agencies contained clauses addressing the key requirements of the PSM, shown in Table 2.1 at page 41. At three of the audited agencies, the model RFT templates examined contained details of, and obliged respondents to adhere to, applicable security requirements. In addition, these model tender templates also contained references to the standards in the PSM and to the respective agencies' security standards, including, for example, security clearance requirements.

2.18 The standard RFT template at the fourth agency did not contain any details of security requirements nor did it contain references to the PSM or the agency's security policies or requirements. That agency was developing, at the time of the audit, an RFT template to better reflect, amongst other things, contemporary security policies and requirements.

2.19 The ANAO found, for the most part, that those model contract templates designed for use in the more-complex and higher-risk procurements (commonly known as long-form contract templates)[16] contained clauses that addressed most of the requirements of the PSM shown in Table 2.1. The main exceptions were that:

- while all the templates contained termination clauses, most did not specifically identify a breach of security requirements as a reason to terminate the contract *(Part F, paragraph 4.17*); and
- most did not contain a clause(s) dealing with the risk of access to the agency's official information through a third party that has, or potentially has, any control or rights over the contractor (*Part F, paragraph 4.8*).

[15] In one agency, the protective security section also provided advice on the development of security-related clauses in tenders and contracts.

[16] Three of the audited agencies also had a range of model contract templates for use in minor, less-complex or lower value procurements. These templates are commonly known as short-form contract templates. Generally, the security requirements in these templates were found to be less extensive than in the long-form templates. The content of these short-form templates was not assessed against the requirements in the PSM.

Procurement planning

2.20 The development, implementation and monitoring of a procurement plan is a central component of an effective procurement exercise. The ANAO expected that procurement planning documentation should have defined the procurement's specifications, and identified and assessed its risks, including security risks. Procurement planning typically also: identifies resource requirements and key stakeholders; provides a timeframe of key deliverables; and recommends the proposed procurement approach.

2.21 At three of the audited agencies, nearly all of the procurement planning documentation examined contained an assessment of the security issues relevant to the proposed procurement. In most cases, the assessment related to whether the contractor(s) would, or may, require access to security classified information, and also considered the attendant security clearance requirements. In those cases where it was relevant, procurement planning also considered: the need for contractors to have security-related qualifications or accreditations; and the security issues involved in the contractor(s) working off-site.

2.22 In the remaining agency, while procurement planning documentation considered a range of pertinent business risks, it did not specifically identify or assess any security-related issues or risks.

Approaching the market

2.23 When approaching the market to invite organisations to bid for contracting work, it is important that documentation associated with the RFT sets out the specific requirements, including any security requirements, relating to the procurement. These documents should also clearly indicate the minimum conditions or criteria prospective contractors are required to meet.

2.24 Across the audited agencies, most of the RFT or equivalent documentation examined during the audit contained references to security requirements relevant to the proposed engagement. Typically this documentation:

- included a reference to the agency's security policies or instructions;

- included references to the minimum standards in the PSM, and where applicable, to the Australian Government Information and Communications Technology Security Manual (ACSI 33);[17]
- indicated that the respondents' compliance with the nominated security requirements was either a condition for participation in the tender or would be assessed as part of the tender evaluation criteria; and
- highlighted that the contractor would, or may, require access to security classified information, and would therefore require a security clearance.

2.25 Amongst those approaches to the market that did not contain any security-related information, nor identify any security requirements, the most noteworthy example related to the provision of security clearance services (albeit for a short period only). Given the nature of the services required in this case, the ANAO considered that a range of security-related requirements should have been included in the approach to the market. This could have included, for example, details of the prospective contractors' security clearances, the security-related accreditations and qualifications of the personnel undertaking the clearances, and details of the physical security controls over the protection of information at the contractor's premises.

2.26 The ANAO acknowledges, however, that in this case the agency obtained a range of additional information prior to finalising its' assessment of the preferred contractors. The ANAO considers this additional information was critical to mitigate the security-risks involved in the proposed contract and to support the agency's assessments concerning the prospective contractors' ability to provide the required services.

[17] ACSI 33, produced by the Defence Signals Directorate, provides policies and guidance to Australian Government agencies on how to protect their information and communications technology systems.

Recommendation No. 1

2.27 To assist staff to manage security risks during procurement and contracting activities, the ANAO recommends that Australian Government agencies:

(a) include in protective security and procurement/contracting policy documents, information on the security risks of using contractors that is appropriate for their operations; and

(b) update model procurement and contract templates to fully reflect the requirements of the PSM (*Part F—Security Framework for Procurement*).

Agencies' responses

Attorney-General's Department, ComSuper and DFAT

2.28 Agreed.

Customs

2.29 Customs agrees with the recommendation. Customs performed satisfactorily against both (a) and (b) of the recommendation and Customs' policy documents are considered to be useful guides to staff in the management of security risks in procurement and contracting activity.

Finance

2.30 Agreed. Finance is currently reviewing and redeveloping security and procurement/contracting policy documentation and procurement and contracting templates.

Evaluating tenders

2.31 The evaluation of tender responses should include an assessment of each prospective contractor's ability to meet relevant security standards. The extent that security issues are considered when evaluating tenders should vary according to the security risks involved in the proposed contract, including whether contractors require access to sensitive or classified information.

2.32 Paragraph 4.3 of the PSM (Part F) requires that procurement evaluation plans properly reflect security requirements contained in the approach to the market. The previous PSM (Part F) contained more detailed guidance to assist agencies satisfy this requirement. For example, paragraph 5.31 of the previous PSM suggested that the following elements could form part of the assessment of security issues during tender evaluation processes:

- personnel: ensuring prospective contractors have relevant skills and experience; hold relevant qualifications and accreditations; and have, or are willing to submit to, a security clearance recognised by the agency;
- facility: assessing the physical security mechanisms and procedures in place at the contractor's premises. This element is particularly relevant in those cases where contractor(s) will be handling and/or storing sensitive or security classified information at their premises; and
- information and communications technology (ICT): assessing the security control framework and operational security controls[18] for the contractors' ICT systems. This may include assessing whether these systems have been certified or accredited in accordance with the standards in ASCI 33. This element is relevant in those cases where official information is to be processed, stored, communicated or otherwise transmitted on, or using the contractor's ICT systems.

2.33 In this regard, the ANAO assessed, for each of the contracts selected for testing:

- the extent that compliance with security requirements was considered in the evaluation of tenders; and
- whether a member of the agency's protective security team, or someone with sufficient knowledge of the security issues involved in the proposed contractual arrangement, was involved in the tender evaluation process.

Confirming compliance with security requirements in the evaluation of tenders

2.34 Across the four audited agencies, the ANAO found that tender evaluation processes had properly considered the security requirements contained in the documentation provided to the market in all but two of the 30 contracts examined in this part of the audit.

2.35 In these two contrasting cases, both approaches to the market contained security requirements related to the fact that the contracted services were to be provided off-site. In both cases, however, the audited agencies relied solely on assurances from prospective contractors that the respective security

[18] The terms 'security control framework' and 'operational security controls' are used to describe the broad components of ICT security. The terms are taken from ANAO Audit Report No.23 2005–2006, *IT Security Management*, December 2005, p. 22.

requirements had been met. The ANAO considered, particularly because the contractors were not to be working under the agencies' direct control, that the agencies should have confirmed through review, or otherwise obtained positive assurance at the time of evaluation, that the security requirements had been adequately met.

Contribution of security expertise to the tender evaluation process

2.36 The evaluation of tender responses should involve officials with a mix of skills and knowledge that are relevant to the function(s) being contracted-out. Depending on the complexity of the issues involved, subject-matter specialists may need to be involved in, or consulted during, evaluation processes. For example, in those cases that involve the evaluation of responses to security-specific standards, agencies might consider including a member of the protective security team, or someone with a sufficient level of knowledge and understanding about those security requirements, on the evaluation team.

2.37 At three of the audited agencies the ANAO found that a member of the agency's protective security team had been involved, or consulted, in many of the tender evaluation processes examined. In the other cases examined at these agencies, the ANAO considered the staff involved in the evaluation process demonstrated a good understanding of the pertinent security issues and requirements. At the fourth agency, there was no evidence that tender evaluation processes had involved a person(s) with knowledge of protective security issues or standards.

2.38 The ANAO considers, particularly for those evaluation processes involving assessments of compliance with specific security requirements, that someone with a sufficient knowledge of these requirements should be involved in, or consulted during, the evaluation process.

Security requirements in contracts

2.39 Contracts form the basis of the relationship between the parties and provide the basis for the control and oversight of the contractor's performance. Australian Government contracts should contain clauses addressing a range of legislative and policy requirements, including details of the contractor's security obligations and a range of other matters contained in the PSM (Part F).

2.40 Table 2.1 outlines key security-related clauses that agencies should include in contracts. It is based on the minimum requirements set out in the relevant paragraphs of Part F of the PSM. The table also reports the ANAO's

findings regarding the extent to which the four audited agencies addressed these issues in the contracts that were examined in the audit.

Table 2.1

Key clauses in contracts relating to security

Contract contains a clause(s):	Number of the 43 tested contracts that met this requirement
Setting out the security requirements and obligations of the contractor. *(PSM, Part F, paragraph 4.5)*	42
Providing that the agency can amend the security requirements during the life of the contract. (*PSM, Part F, paragraph 4.5)*	34
Providing reasonable access, for both the agency and the ANAO, to the contractor's premises, records and equipment. *(PSM, Part F, paragraphs 4.10 and 4.18)*	40
Requiring the contractor to consult before sub-contracting any of the functions covered by the contract, particularly any functions requiring access to security classified or sensitive information. *(PSM, Part F, paragraph 4.16)*	40
Making the contractor responsible for ensuring that any sub-contractors fully meet all security requirements in the contract. *(PSM, Part F, paragraph 4.15)*	37
Requiring the contractor to implement procedures designed to restrict access to the agency's security classified information to those employees who have the appropriate security clearance and who require access to perform their work. *(PSM, Part F, paragraph 4.14)*	37
Dealing with the risk of access to the agency's information through a third party that has, or potentially has, any control or rights over a contractor. *(PSM, Part F, paragraph 4.8)*	24
Identifying that the contract will/may be terminated for failure to comply with the security requirements. (*PSM, Part F, paragraph 4.17*)	23(1)

Notes: (1) While all the contracts had termination clauses, only 23 specifically identified a breach of security requirements as a reason for terminating the contract.

Source: ANAO, based on Part F of the PSM.

2.41 Overall, the ANAO found that most of the contracts examined addressed most of these requirements. In particular, with only one exception,

all of the contracts examined contained clauses setting out the security requirements and obligations related to the contracted function(s).[19]

2.42 However, the security requirements contained in the contracts examined varied widely. They ranged from, in a few cases, a general requirement to comply with security directions to, also in a few cases, very-detailed and specific requirements relating to the function being contracted-out. The security requirements in the contracts examined typically included the need for the contractor(s) to:

- comply with the minimum standards in the PSM and the agencies' own security policies or instructions;
- undertake security training;
- obtain a security clearance;
- participate in security reviews or audits, if requested;
- provide details of any security incidents;
- advise of any changes in the personal circumstances of specified personnel;
- provide reports on security matters, including details of perceived problems and recommendations for improvement; and
- maintain relevant security accreditations.

2.43 In addition, most of the contracts also stated that security requirements could be amended during the life of the contract. All of the contracts that did not explicitly state that security requirements could be amended during the life of the contract related to one agency. During the audit, the ANAO observed that this agency has included such a clause in its recently promulgated model 'long-form' contract template. This is expected to result in the consistent use of such a clause in the agency's contracts in the future.

2.44 Despite the reasonably comprehensive coverage of security requirements in most of the contracts examined, around half of the contracts examined did not:

- contain a clause(s) dealing with the risk of access to the agency's information through a third party that has, or may have, any control or

[19] The contract that did not contain any security provisions is due to expire during 2007. At the time of the audit, the relevant agency advised that it was formalising the security obligations to be contained in the proposed new contract as part of preparing a RFT.

rights over the contractor.[20] The ANAO expected that all the contracts examined would have included such a clause(s) because there was no evidence that the existence, or absence, of such rights or controls was considered during tender evaluation or contract negotiation activities; and

- specifically identify a failure to meet security requirements as a reason to terminate the contract.[21] The ANAO considers identifying non-compliance with security obligations as an explicit reason to terminate a contract to be a useful way to emphasise the importance of security-matters to contractors. Given the nature of the services provided under the contracts examined during the audit, the ANAO considered that all of the contracts should have explicitly mentioned that the contract could be terminated for a failure to comply with security requirements.

2.45 One of the reasons why a number of the contracts examined did not contain these two clauses is likely to be that most of the audited agencies' model contract templates did not contain these clauses (see paragraph 2.19). The implementation of the ANAO's recommendation to enhance, as necessary, contract templates to better reflect the requirements of the PSM, should result in agencies more frequently including these two clauses in contracts.

[20] Paragraph F4.8 of the PSM requires that agencies should consider the risks of access to their information through any third party interests or rights regarding contractors, and as considered necessary, address this matter in the contract.

[21] Paragraph F4.17 of the PSM indicates that agencies should have the ability to terminate a contract for security breaches committed by the contractor, or due to the contractors' inability to remedy those breaches.

3. Managing Security Issues in Contracting

This chapter discusses the audit findings and better practices identified in the audited agencies relating to managing security issues after a contract has been signed. It examines: the provision of security-related training to contractors; managing the contractor's performance, including adherence to relevant security requirement; and the mechanisms used to identify, report and record the details of any security breaches by contractors.

Orientation and training

Introduction

3.1 Providing employees and contractors, particularly those with access to an agency's sensitive and security classified information, with security awareness training is an important part of good security management and an essential tool in minimising security risks. Well-designed security awareness training can assist foster a strong security culture by:

- promoting understanding about an agency's protective security policies and procedures;
- providing clarity on security-related requirements and responsibilities; and
- highlighting the risks of poor security practice.

3.2 The importance of promoting security awareness is highlighted throughout the PSM.[22]

3.3 To assess the adequacy of the orientation and training of contractors about security issues, the ANAO evaluated, at each of the audited agencies:

- methods to promote security awareness amongst contractors;
- whether security awareness training is designed to provide contractors with details of the agency's protective security policies;
- whether the content of security awareness training accorded with selected requirements in the PSM; and

[22] For example, it is discussed at: Part C (information security), paragraph 3.15; Part D (personnel security), paragraphs 10.41-42; Part E (physical security), paragraph 3.13; and Part G (security incidents), paragraph 3.9.

- for each of the contracts selected for testing, whether the specified contractor(s) had attended security awareness training.

Promoting security awareness

3.4 To support the establishment and maintenance of a strong security culture, agencies need a program to regularly and consistently promote security awareness across each of the dimensions of protective security.

3.5 The ANAO found that each of the audited agencies regularly provides formal security awareness training for 'new starters'. At one agency, however, contractors were not required to attend the security awareness training provided to 'new starters'. This agency advised that some contractors may have been provided with briefings on security requirements relevant to their engagement prior to their engagement. However, the agency provided no evidence of this, or of the nature of the briefings. To strengthen its' security awareness training arrangements, this agency advised the ANAO that it planned, in the future, to provide security awareness briefings to all new contractors prior to their commencing work. At another agency, the attendance of new contractors' at security awareness training was only made mandatory from November 2006.

3.6 As well as providing security awareness training, a number of other good practices for promoting security awareness were observed at the audited agencies. These included:

- two agencies supplemented formal security awareness training with work-area specific induction arrangements;
- two agencies required all staff and contractors to attend formal security awareness refresher training courses; and
- one agency required all staff and contractors to acknowledge, in writing each year, their responsibilities in a range of security-related matters, including:
  - notifying changes in personal circumstances;
  - reporting breaches of security; and
  - handling and disposing of documents.

3.7 In addition, at the time of the audit, two of the agencies were considering using on-line security questionnaires to periodically assess the security awareness of contractors.

Content of security awareness training

3.8 Table 3.1 outlines the core content that agencies should include in security awareness training programmes for contractors. It is based on the minimum requirements contained in Parts C, D, F and G of the PSM. The table also reports the ANAO's findings of the extent to which the four audited agencies covered these issues in their security awareness training programmes for contractors.

Table 3.1

Core content of security awareness training

Security awareness issues that contractors are advised about in training:	Number of the four audited agencies that addressed this element
Their responsibility for keeping the entity informed of security incidents. (*PSM, Part G, paragraph 3.6 and Part F, paragraph 4.19)*	4 although at one agency the training only covered the management of ICT security incidents
Close of business standards and procedures. *(PSM, Part C, paragraph 7.8)*	4
Standards for storing security classified information, including the types of container to be used. *(PSM, Part C, paragraphs 7.42)*	3
Standards for transmitting security classified information. *(PSM, Part C, paragraphs 7.43 to 7.72)*	3
How to determine the appropriate security classification to be placed on information. *(PSM, Part C, paragraphs 6.12 and 6.31 to 6.43)*	4 although at one agency the training only addressed the use of security classifications in relation to e-mails
The use of protective markings. *(PSM, Part C, paragraph 6.28)*	4 although at one agency the training only addressed the use of protective markings on e-mails
Their responsibility for notifying the entity about changes in personal circumstances that may affect their security clearance. *(PSM, Part D, paragraph 10.26)*	3

Source: ANAO, based on the PSM.

3.9 Overall, the ANAO found that the audited agencies were delivering security awareness training programmes that addressed most of the key security issues to contractors. For example, the training at each agency explained the reasons why security awareness was important, promoted an

understanding of the agency's security policies, and provided clarity on attendant roles and responsibilities.

Attendance of contractors at security awareness training

3.10 Security awareness training will not be effective in managing security risks associated with contractors, unless most, if not all, contractors are required to attend it.

3.11 At the time of the audit, the audited agencies had a range of processes for identifying new starters, including contractors, required to attend security awareness training. For example, in one agency, all new starters were notified, by email, of the agency's mandatory training requirements, including security awareness training. At these agencies, new staff and contractors were advised of the need to attend security awareness training either when they obtained their building access-pass or when they received confirmation of their security clearance.

3.12 Each of the audited agencies also maintained records of the staff and contractors attending security awareness training. A sound and better practice observed at one agency was the inclusion of details of attendance (and non-attendance) at security awareness training in reports to the agency's executive.

3.13 The ANAO's testing has indicated, however, that a significant number of contractors engaged under the contracts being examined at the audited agencies may not have attended security awareness training. At one agency, for example, attendance records indicated that most of the contractors currently working under the contracts examined had not attended security awareness training. At the agency that only introduced mandatory security awareness training for contractors in late-2006, there was no evidence to indicate that any of the contractors working on the contracts examined had attended security awareness training. Discussions with contract managers at this agency indicated that it was likely that none of these contractors had attended such training.

3.14 At the remaining two agencies, the review of attendance records suggested that most, but not all, of the contractors working for the agencies under the contracts selected for testing had attended security awareness training.

Managing contractors' performance, including adherence to security requirements

3.15 It is important that contracts are actively managed throughout their life to help ensure contractors' performance is satisfactory, stakeholders are well informed, and all contract requirements are met.[23]

3.16 Australian Government agencies remain accountable for the performance of all contracted services or functions. This includes ensuring that the work is undertaken in accordance with the requirements contained in a wide-range of Australian Government general policies, including the PSM. To gauge the performance of each of the audited agencies in managing ongoing security risks associated with contractors, the ANAO evaluated, for each of the selected contracts, whether:

- the audited agencies were regularly monitoring the performance of the contractor, including adherence to security requirements;
- security issues and risks identified during procurement planning have been reassessed during the life of the contract to ascertain if they remain appropriate and relevant; and
- contractors were involved in any recent security incidents.

Monitoring contractors' performance

3.17 Regular monitoring and review of contractors' performance can be a key element of an agency's continuous improvement process. Regular monitoring can facilitate the prompt identification of potential security weaknesses relating to contractors and assist in the timely implementation of remedial treatments.

3.18 The nature of contract management processes should depend on the relative size, complexity, and risks involved in each contract. The ANAO's Better Practice Guide *Developing and Managing Contracts* identifies the following factors as important when determining the nature of contract management processes: strategic importance of the contracted services; extent of impact on stakeholders; value of the contract; security requirements; and the experience of contractor staff.[24]

---

[23] ANAO, *Better Practice Guide: Developing and Managing Contracts—Getting the Right Outcome, Paying the Right Price*, op. cit., p. 72.

[24] ibid., p. 44.

3.19 The PSM indicates that as well as monitoring performance, contract management processes should involve monitoring adherence to the security obligations specified in the contract. Part F of the previous PSM contained more-specific information in this area and suggested that the following mechanisms should form part of the framework for monitoring the security-related performance of contractors:[25]

- clarity in the contract as to the security requirements and standards applying to the contractor;
- establishing a project officer with clearly defined responsibilities;
- the provision of regular reports on security performance;
- conducting regular security inspections; and
- requiring contractors to report details of any security incidents relevant to the contract.

Clauses in contracts concerning contractor's performance

3.20 The ANAO found, in three of the audited agencies, that nearly all the contracts reviewed contained a clause(s) relating to the management of the contractor's performance. In the fourth agency, only four of the 13 contracts reviewed contained such a clause(s).

3.21 For the most part, the contract management provisions in the contracts examined related to the provision of reports on, and the conduct of regular meetings about, the services being provided. In one agency, all of the contracts examined also contained schedules of performance indicators or service levels, including security. Specifically, in relation to managing the security-related performance of contractors, the ANAO found the following good practices:

- several of the contracts examined at one agency listed penalties (other than terminating the contract) for the failure to meet security requirements;
- at one agency, all of the contracts provided that contractors must submit security reports and participate in security reviews, when requested to do so;
- at two agencies, five of the contracts examined required the contractor to submit regular reports on security progress or performance; and

[25] See PSM paragraphs 5.41, 6.8, 6.16–17 and 6.19.

- six of the contracts examined at one agency required contractors to participate, at least annually, in reviews of the operation of security requirements.

Mechanisms to manage the performance of contractors

3.22 Across the four audited agencies, the ANAO observed a variety of mechanisms to manage the performance of contractors. This included holding regular meetings, reviewing status reports, inspecting work and, in a few cases, monitoring results against service standards or key performance indicators. However, the use of such systematic mechanisms was not common or consistent. For the most part, contract management processes, including the management of security issues, tended to be informal, unstructured and were often undocumented.

3.23 There was no evidence, for most of the contracts reviewed, that agencies were regularly assessing contractors' adherence to security requirements. For example, the ANAO identified that agencies systematically assessed security performance, or measured compliance with security requirements, in only seven of the 43 contracts examined in this part of the audit. The audited agencies typically advised the ANAO that security matters were only considered if, and when, matters arose. Some of the contract managers interviewed during the audit also suggested that they relied on the agency's broader security functions and policies to provide them with assurance that contractors were complying with security requirements.

3.24 In those cases where contractors worked under direction or control, contract managers across the four audited agencies indicated that performance, including security issues, was generally monitored through observation and discussion, as part of ongoing supervision and oversight. The ANAO considers this to be a reasonable approach. However, in those cases where contractors do not work under direct or ongoing supervision, the ANAO considers that contract managers should implement processes to obtain assurance about the performance of contractors, including their compliance with security requirements.

Review of security risks and requirements

3.25 Reviewing security risks during the life of certain contracts can be important as it enables an agency to identify risks that may have escalated beyond their originally assessed level and also to identify any new and emerging risks. In particular, the ANAO considers that security risks involved

with high-value or high-risk contracts should be reviewed whenever there is a significant change in the circumstances associated with the contract, or when a contract is extended significantly beyond its original term.

3.26 While each of the audited agencies required risk assessments to be undertaken to support spending proposals related to contract extensions, none specifically addressed, in relevant policy documents, the need to consider security issues in the conduct of these assessments. In addition, none of the agencies had policies requiring security risks to be reviewed when there has been a change in a contract's circumstances that is likely to affect these risks.

3.27 One of the audited agencies had a formal and regular process to measure security risks and identify potential security deficiencies across a broad-range of elements in its operational environment. However, while this process captures details of the number of contractors engaged by the agency, it did not, at the time of the audit, obtain other information that the ANAO considers would contribute to an assessment about the status of security risks involving the use of contractors.[26]

3.28 Of the 43 contracts examined in this part of the audit, the ANAO found that fourteen had either been extended beyond their original term, or the services being provided had been affected by a significant change in circumstances. In only half of these cases was the decision to extend or continue the contractual arrangement supported by a re-assessment of the security risks and requirements involved.

Recommendation No. 2

3.29 As part of ongoing contract management, the ANAO recommends that Australian Government agencies adopt a risk-based approach to monitoring and evaluating the performance of contractors, including their adherence to security requirements. This approach should require agencies to re-evaluate security risks of contracts that are affected by a significant change in circumstances, or which are extended significantly beyond their original term.

Agencies' responses

Attorney-General's Department, ComSuper, DFAT and Finance

3.30 Agreed.

[26] This agency agreed to expand this tool to capture more pertinent information for assessing changes in security risks involved in the use of contractors.

Customs

3.31 Customs agrees with the recommendation. Customs has appropriate procedures and processes in place that ensures a risk-based approach to monitoring and evaluating the performance of contractors.

Security incidents

3.32 One objective of managing security risks in contracting is to minimise the frequency and impact of security breaches by contractors without detracting from the cost-effective delivery of services. The effective management of security incidents involves having policies and practices to identify, report and record the details of all incidents. In addition, appropriate remedial action should be taken to minimise the impact, and to prevent the re-occurrence, of further security incidents.

3.33 The PSM (Part G) contains guidance, and minimum standards, relating to the management of security incidents by Australian Government agencies. Specifically, it highlights that agencies must have processes for identifying and dealing with security incidents involving the performance of contracted functions.

3.34 Most of the contracts the ANAO examined contained a clause(s) requiring the contractor to advise the respective agency of the details of any security incidents. In addition, security awareness training programmes in each of the audited agencies provided information about reporting security incidents.

3.35 The ANAO found that three of the audited agencies had systems for identifying, recording and monitoring details of security breaches or security incidents. In the fourth agency, although policy documents required details of information and communications technology security incidents to be reported to relevant staff, the agency did not have a system for effectively capturing such details.

3.36 The ANAO found only one record of a recent security incident involving a contract examined during the audit. In this case, the ANAO considered that the agency responded quickly and appropriately to the incident. The actions taken not only minimised potential risks at the time, but were designed to reduce the likelihood of similar incidents occurring again.

3.37 While this result suggests the contractors involved with the contracts examined have largely adhered to security requirements, the ANAO notes that security breaches may not always be reported. In addition, as mentioned above, one of the audited agencies did not have a system to effectively monitor and report such incidents.

Ian McPhee
Auditor-General

Canberra ACT
13 June 2007

Appendices

Appendix 1: Agency comments

Each of the audited agencies, together with the Attorney-General's Department, were provided with the opportunity to comment on the proposed audit report in accordance with section 19 of the *Auditor-General Act 1997*.

Agencies' responses to the recommendations have been included in Chapters 2 and 3 of the report directly following each recommendation. Other general comments are reproduced below.

Attorney-General's Department (AGD)

AGD advised as follows:

> I note the recommendations require greater adherence to the Protective Security Manual provisions, particularly with respect to ongoing management of contracts. This issue was highlighted in the 2005 Australian Government Protective Security Survey which identified deficiencies in monitoring compliance with security requirements during the contract. The 2006 Survey has sought more detail relating to contracts, with the results of the survey expected to be submitted to Government in late 2007.

Commonwealth Superannuation Administration (ComSuper)

ComSuper advised as follows:

> ComSuper acknowledges the outcomes of the report and supports the findings. ComSuper has recently commenced a number of process and policy improvements around our compliance with the Protective Security Manual, including the engagement of an Agency Security Advisor to assist us in delivering on these outcomes. ComSuper confirms that we will be implementing changes to our processes and policy framework to reflect the ANAO's recommendations.

Australian Customs Service (Customs)

Customs advised as follows:

> Customs agrees with the key findings and conclusions and notes that the ANAO assessed Customs as being satisfactory against all the audit criteria and that Customs performed well in a number of aspects.

Department of Foreign Affairs (DFAT)

DFAT advised as follows:

> As has been acknowledged by the ANAO, DFAT is managing effectively security risks involved in the use of contractors. However, DFAT recognises that there is scope for improvement. We are currently reviewing our security arrangements for contractors and looking at ways of improving management of various contracts that contain a significant security element.

Department of Finance and Administration (Finance)

Finance advised as follows:

> Finance supports the recommendations contained in the proposed report.

Appendix 2: Protective Security Audits

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

- Audit Report No.21, 1996–1997, *Protective Security;*
- Audit Report No.7, 1999–2000, *Operation of the Classification System for Protecting Sensitive Information;*
- Audit Report No.22, 2001–2002, *Personnel Security—Management of Security Clearances;*
- Audit Report No.23, 2002–2003, *Physical Security Arrangements in Commonwealth Agencies;*
- Audit Report No.55, 2003–2004, *Management of Protective Security;*
- Audit Report No.41, 2004–2005, *Administration of Security Incidents, including the Conduct of Security Investigations; and*
- Audit Report No.23, 2005–2006, *IT Security Management.*

Index

Series Titles

Audit Report No.1 Performance Audit
Administration of the Native Title Respondents Funding Scheme
Attorney-General's Department

Audit Report No.2 Performance Audit
Export Certification
Australian Quarantine and Inspection Service

Audit Report No.3 Performance Audit
Management of Army Minor Capital Equipment Procurement Projects
Department of Defence
Defence Materiel Organisation

Audit Report No.4 Performance Audit
Tax Agent and Business Portals
Australian Taxation Office

Audit Report No.5 Performance Audit
The Senate Order for the Departmental and Agency Contracts (Calendar Year 2005 Compliance)

Audit Report No.6 Performance Audit
Recordkeeping including the Management of Electronic Records

Audit Report No.7 Performance Audit
Visa Management: Working Holiday Makers
Department of Immigration and Multicultural Affairs

Audit Report No.8 Performance Audit
Airservices Australia's Upper Airspace Management Contracts with the Solomon Islands Government
Airservices Australia

Audit Report No.9 Performance Audit
Management of the Acquisition of the Australian Light Armoured Vehicle Capability
Department of Defence
Defence Materiel Organisation

Audit Report No.10 Performance Audit
Management of the Standard Defence Supply System Remediation Programme
Department of Defence
Defence Materiel Organisation

Audit Report No.11 Performance Audit
National Food Industry Strategy
Department of Agriculture, Fisheries and Forestry

Audit Report No.12 Performance Audit
Management of Family Tax Benefit Overpayments

Audit Report No.13 Performance Audit
Management of an IT Outsourcing Contract Follow-up Audit
Department of Veterans' Affairs

Audit Report No.14 Performance Audit
Regulation of Pesticides and Veterinary Medicines
Australian Pesticides and Veterinary Medicines Authority

Audit Report No.15 Financial Statement Audit
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2006

Audit Report No.16 Performance Audit
Administration of Capital Gains Tax Compliance in the Individuals Market Segment
Australian Taxation Office

Audit Report No.17 Performance Audit
Treasury's Management of International Financial Commitments—Follow-up Audit
Department of the Treasury

Audit Report No.18 Performance Audit
ASIC's Processes for Receiving and Referring for Investigation Statutory Reports of Suspected Breaches of the Corporations Act 2001
Australian Securities and Investments Commission

Audit Report No.19 Performance Audit
Administration of State and Territory Compliance with the Australian Health Care Agreements
Department of Health and Ageing

Audit Report No.20 Performance Audit
Purchase, Chartering and Modification of the New Fleet Oiler
Department of Defence
Defence Materiel Organisation

Audit Report No.21 Performance Audit
Implementation of the revised Commonwealth Procurement Guidelines

Audit Report No.22 Performance Audit
Management of Intellectual property in the Australian Government Sector

Audit Report No.23 Performance Audit
Application of the Outcomes and Outputs Framework

Audit Report No.24 Performance Audit
Customs' Cargo Management Re-engineering Project
Australian Customs Service

Audit Report No.25 Performance Audit
Management of Airport Leases: Follow-up
Department of Transport and Regional Services

Audit Report No.26 Performance Audit
Administration of Complex Age Pension Assessments
Centrelink

Audit Report No.27 Performance Audit
Management of Air Combat Fleet In-Service Support
Department of Defence
Defence Materiel Organisation

Audit Report No.28 Performance Audit
Project Management in Centrelink
Centrelink

Audit Report No.29 Performance Audit
Implementation of the *Sydney Airport Demand Management Act 1997*

Audit Report No.30 Performance Audit
The Australian Taxation Office's Management of its Relationship with the Tax Practitioners: Follow-up Audit
Australian Taxation Office

Audit Report No.31 Performance Audit
The Conservation and Protection of National Threatened Species and Ecological Communities
Department of the Environment and Water Resources

Audit Report No.32 Performance Audit
Administration of the Job Seeker Account
Department of Employment and Workplace Relations

Audit Report No.33 Performance Audit
Centrelink's Customer Charter–Follow-up Audit
Centrelink

Audit Report No.34 Performance Audit
High Frequency Communication System Modernisation Project
Department of Defence
Defence Materiel Organisation

Audit Report No.35 Performance Audit
Preparations for the Re-tendering of DIAC's Detention and Health Services Contracts
Department of Immigration and Citizenship

Audit Report No.36 Performance Audit
Management of the Higher Bandwidth Incentive Scheme and Broadband Connect Stage 1
Department of Communications, Information Technology in the Arts

Audit Report No.37 Performance Audit
Administration of the Health Requirement of the Migration Act 1958
Department of Immigration and Citizenship
Department of Health and Ageing

Audit Report No.38 Performance Audit
Administration of the Community Aged Care Packages Program
Department of Health and Ageing

Audit Report No.39 Performance Audit
Distribution of Funding for Community Grant Programmes
Department of Families, Community Services and Indigenous Affairs

Audit Report No.40 Performance Audit
Centrelink's Review and Appeals System Follow-up Audit
Centrelink

Audit Report No.41 Performance Audit
Administration of the Work for the Dole Programme
Department of Employment and Workplace Relations

Audit Report No.42 Performance Audit
The ATO's Administration of Debt Collection—Micro-business
Australian Taxation Office

Current Better Practice Guides

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

Administering Regulation	Mar 2007
Developing and Managing Contracts	
Getting the Right Outcome, Paying the Right Price	Feb 2007
Implementation of Programme and Policy Initiatives:	
Making implementation matter	Oct 2006
Legal Services Arrangements in Australian Government Agencies	Aug 2006
Preparation of Financial Statements by Public Sector Entities	Apr 2006
Administration of Fringe Benefits Tax	Feb 2006
User–Friendly Forms Key Principles and Practices to Effectively Design and Communicate Australian Government Forms	Jan 2006
Public Sector Audit Committees	Feb 2005
Fraud Control in Australian Government Agencies	Aug 2004
Security and Control Update for SAP R/3	June 2004
Better Practice in Annual Performance Reporting	Apr 2004
Management of Scientific Research and Development Projects in Commonwealth Agencies	Dec 2003
Public Sector Governance	July 2003
Goods and Services Tax (GST) Administration	May 2003
Managing Parliamentary Workflow	Apr 2003
Building Capability—A framework for managing learning and development in the APS	Apr 2003
Internal Budgeting	Feb 2003
Administration of Grants	May 2002
Performance Information in Portfolio Budget Statements	May 2002
Life-Cycle Costing	Dec 2001
Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	June 2001

Internet Delivery Decisions	Apr 2001
Planning for the Workforce of the Future	Mar 2001
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Commonwealth Agency Energy Management	June 1999
Security and Control for SAP R/3	Oct 1998
New Directions in Internal Audit	July 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