

The Auditor-General
Audit Report No.41 2004–05
Protective Security Audit

Administration of Security Incidents, including the Conduct of Security Investigations

© Commonwealth
of Australia 2005

ISSN 1036-7632

ISBN 0 642 80838 4

COPYRIGHT INFORMATION

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth available from the Department of Communications, Information Technology and the Arts.

Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration,
Attorney-General's Department,
Robert Garran Offices,
National Circuit
Canberra ACT 2600

[http://www. ag. gov. au/cca](http://www.ag.gov.au/cca)



Canberra ACT
15 April 2005

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a protective security audit in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit and the accompanying brochure. The report is titled *Administration of Security Incidents, including the Conduct of Security Investigations*.

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

Yours sincerely

A handwritten signature in black ink, appearing to read 'Ian McPhee', is positioned above the printed name and title.

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

Russell Coleman
Bill Bonney
Amali Bandara
Ewan Windsor

Contents

Abbreviations/Glossary.....	6
Summary and Recommendations	9
Summary	11
Background	11
Audit objective	12
Audited entities	12
Audit conclusion	12
Recommendations	13
Responses provided by entities	13
Sound and better practices	13
Recommendations.....	15
Audit Findings and Conclusions	19
1. Introduction.....	21
Protective security	21
Protective security audits by the ANAO	22
Security incidents and investigations	23
Protective Security Manual.....	23
Audit objective and criteria	24
Audit coverage	24
Structure of the report	25
2. Management Framework	26
Introduction.....	26
Policy and procedures.....	26
Training and awareness.....	30
Monitoring and reporting security incident and investigation information	33
3. Security Incidents and Investigations	36
Introduction.....	36
Recording details of security incidents.....	38
Conduct of security investigations.....	42
Appendices	47
Appendix 1: Audit Criteria.....	49
Appendix 2: Entities' responses to the audit report.....	50
Index	52

Abbreviations/Glossary

ANAO	Australian National Audit Office
APS	Australian Public Sector
ASA	Agency Security Adviser
ASIO	Australian Security Intelligence Organisation
Contact	An unsolicited encounter with people or organisations that may be an attempt to obtain security or official information they do not have a need to know.
DSD	Defence Signals Directorate
Audit criteria	Normative or desirable controls or processes (that are at reasonable and attainable standards) against which the subject matter under review is assessed.
ISIDRAS	Information Security Incident Detection, Reporting and Analysis Scheme
IT	Information Technology
Protective security	A broad concept covering information, personnel, physical and information technology and telecommunications security.
PSM	Protective Security Manual
Security awareness	Understanding or appreciating the potential risks and threats to, and the costs of, the loss or compromise of information or assets, and accepting the responsibilities and obligations to address those issues.
Security incident	A security breach, violation, contact or approach from those seeking unauthorised access to official resources, or any other occurrence that results in negative consequences for the Australian Government.

Security investigation	An investigation carried out to establish the cause and extent of a security incident that has or could have compromised the Australian Government. The overall purpose of a security investigation is to prevent the incident from happening again by making improvements to the agency's systems or procedures.
Sound and better practices	Business practices, which, if adopted, would strengthen the internal control framework and lead to improved operational effectiveness and efficiency.

Summary and Recommendations

Summary

Background

1. The effective administration of security incidents and investigations is a fundamental part of good security management. Information gathered on security incidents and investigations may highlight the need for entities¹ to re-assess the adequacy of current practices or arrangements, and is also a key input into continuous improvement activities. In turn, good security management helps to contain the effects of a security incident and enables entities to manage the consequences of a security incident and to recover as quickly as possible.²
2. Entities can encounter a wide-range of security incidents including the theft or loss of assets, the inappropriate handling or suspected compromise of classified information, instances of unauthorised access to information or restricted work areas and the physical or threatened assault of staff. The number and type of security incidents generally reflect the nature of each entity's work, including the level of classified or sensitive information. It may also be influenced by such factors as, the conduct of regular security inspections, the strength of security awareness amongst staff, and the ease of reporting security incidents.
3. The Protective Security Manual (PSM), issued by the Attorney-General, is the principal source of protective security policies, principles and standards for Australian Government entities.³ Part G of the PSM contains instructions and guidance on the administration of security incidents and investigations.

¹ In this report, the term 'entity' is used to describe any Australian Government body, including those organisations subject to the *Financial Management and Accountability Act (FMA Act) 1997* and the *Commonwealth Authorities and Companies Act (CAC Act) 1997*.

² Australian Security Industry Forum – Security 2004, *Opening Address – Security in a Changing Environment*, Attorney-General, 14 July 2004, Sydney.

³ Legal advice obtained by the Attorney-General's Department indicates that CAC Act entities do not have to comply with the PSM unless specifically directed to do so by their Minister. Nevertheless, the ANAO considers adoption of the measures contained in the PSM, where cost effective, to be good protective security practice.

Audit objective

4. The objective of the audit was to evaluate the policies and practices of selected Australian Government entities to determine whether they had established robust arrangements for, and maintained effective control over, the administration of security incidents and investigations.

Audited entities

5. The following entities participated in the audit:

- Australian Crime Commission;
- Australian Customs Service;
- Australian Maritime Safety Authority;
- Child Support Agency; and
- Department of Finance and Administration.

Audit conclusion

6. Overall, the ANAO concluded that the audited entities had sound policies and practices in place to support, and maintain effective control over, the administration of security incidents and the conduct of security investigations. In particular, the audit found that most of the entities had established sound processes for capturing and recording security incidents.

7. The audit also considered that the experience and training of key security-staff, together with good levels of support by management, contributed positively to the effective administration of security incidents and investigations in the audited entities.

8. However, the ANAO did identify a number of shortcomings, and opportunities for further improvement, in policies and practices around the administration of security incidents. These matters mainly relate to:

- improving the content, and processes for maintaining the currency of, security-related policy and procedural documentation;
- developing a formal plan or strategy to assist with the management of security awareness activities;
- establishing more formal (and regular) processes for the review, analysis and reporting of the impact of security incidents and investigations on the security health of the entity;

- providing greater clarity and accountability for decisions on the responses taken to security incidents, including the decision to undertake a security investigation; and
- putting in place mechanisms to improve the communication of information between different work areas involved in security or security-related investigations.

Recommendations

9. The ANAO has made seven recommendations based on the findings from the entities reviewed. These recommendations are likely to have relevance to the administration of security incidents in all Australian Government entities.

Responses provided by entities

10. Each of the audited entities, together with the Attorney-General's Department,⁴ has indicated that they agree with the audit recommendations.

Sound and better practices

11. The following table highlights examples of sound and better practices observed in the audited entities.

⁴ The Attorney-General's Department was provided the opportunity to comment on the report given its central policy role in relation to protective security.

Table 1

Sound and better practices in relation to the administration of security incidents

Management Framework	
Policies and procedures	A staff feedback scheme, with a hyper-link embedded in each policy document, gives staff the opportunity to provide feedback on the policy. All submissions are logged in a database and are provided to the relevant area for consideration.
Training and awareness	<p>Staff are assessed against a range of security awareness competencies, including demonstrating an awareness and understanding of personal security obligations, as part of the performance assessment process.</p> <p>The use of an on-line learning package, with tailored modules depending on the security level of staff.</p> <p>The distribution to all staff of a brochure covering all elements of security.</p>
Monitoring and reporting security incident and investigation information to management	<p>Policy and procedural documentation highlights that incident reports should be regularly evaluated as part of continuous improvement activities, in particular to assess:</p> <ul style="list-style-type: none"> - the implications for operating procedures; - if the level of security risk is increasing; - potential OH&S implications; and - the need for new policy and procedures.
Security Incidents and Investigations	
Recording security incident details	<p>The conduct of regular random security inspections as a pro-active means of managing the risk of breaches of information security requirements.</p> <p>The existence of a flowchart on security incident reporting that leads staff through the actions required, and demonstrates the support that can be expected from their supervisor or team leader.</p>

Source: ANAO, based on audited entities' information

Recommendations

The following recommendations are based on the findings of the fieldwork at the audited entities. The ANAO considers that they are likely to be relevant to all entities in the Australian Government Sector. All entities should therefore assess the benefits of implementing the recommendations in light of their own circumstances, including the extent to which each recommendation, or part thereof, is addressed by processes and controls already in place.

Recommendation No.1

Para 2.10

Policies and procedures

The ANAO recommends that documentation relating to the administration of security incidents and the conduct of security investigations should, at a minimum:

- specify the roles and responsibilities of staff involved in the administration of security incidents and the conduct of security investigations; and
- include the following information:
 - a definition of a security incident and the types of security incidents common to the entity;
 - guidance on reporting security incidents internally, and to relevant external parties;
 - guidance for investigating security incidents, including distinguishing between the actions required for security investigations, and investigations into matters not related to security; and
 - a nominated ‘owner’ and their responsibilities, and the processes for maintaining the currency of the documents.

Recommendation No.2
Para 2.24
Security awareness

The ANAO recommends that entities develop a formal plan or strategy for the management and delivery of their security awareness activities.

Recommendation No.3
Para 2.38
Monitoring and reporting security incident and investigation information

The ANAO recommends that entities regularly monitor security incident records and investigations reports, and incorporate an analysis of the impact of security incidents in reports to senior management.

Recommendation No.4
Para 3.17
Security inspections

The ANAO recommends that entities consider implementing a program of security inspections, in light of the risks of the loss, or compromise, of their information holdings or other assets.

Recommendation No.5
Para 3.26
Reporting and recording security incidents

The ANAO recommends that entities develop appropriate processes for the consistent and timely reporting and recording of security incident details, including an assessment of the consequences of each incident.

**Recommendation
No.6**

Para 3.41

**Responding to
security incidents**

The ANAO recommends that:

- responsibility for deciding on responses to security incidents be clearly assigned to individual managers or work areas;
- decisions on the response to be taken on each security incident be properly documented; and
- summary details of responses to security incidents be included in management reports.

**Recommendation
No.7**

Para 3.53

**Security
investigations**

The ANAO recommends that entities establish formal mechanisms for communicating information between security staff and other work areas involved in security or security-related investigations.

Responses provided by entities

12. Each of the audited entities, together with the Attorney-General's Department, has indicated that they agree with the audit recommendations.

13. Entities' responses to the recommendations are shown following each recommendation in Chapters 2 and 3. Other general comments provided by the entities are shown at Appendix 2.

Audit Findings and Conclusions

1. Introduction

This chapter provides background information about the audit, including an overview of the ANAO's Protective Security audit program, and details of the objective and scope of the audit.

Protective security

1.1 Protective security broadly describes the policies and practices used by entities to protect their resources. It encompasses the following aspects:

- physical security – building access controls and processes (both into and within the office), including guard stations, access-control devices, alarm systems and the use of secure storage containers;
- administrative or information security – restricting access to, and the distribution of, information through the application of classified markings;
- personnel security – processing security clearances for those staff with the need for access to classified and official information or resources and the maintenance of security awareness levels; and
- information technology – protecting the integrity of electronic information and business systems through, for example, logical access controls and data storage and transmission controls.

1.2 As noted in Audit Report No.55, 2003–2004, *Management of Protective Security*⁵ these elements need to be subject to robust oversight and coordination to help ensure they are delivered in a consistent and complimentary manner. Entities also need to be alert to the implications of any weaknesses or risks in any one area of protective security on controls in another area.

1.3 The management of protective security should not be undertaken in isolation. It should, together with other critical functions, such as business continuity planning and risk management, form a key element of each entity's governance framework.

⁵ Australian National Audit Office (2004), *Management of Protective Security*, Audit Report No.55, 2003–2004, Canberra, p. 18.

Protective security audits by the ANAO

1.4 Since 1995, the ANAO has conducted a series of audits of protective security arrangements as part of its general performance audit program. This series comprises the following reports:

- *Protective Security* – Audit Report No.21, 1996–1997;
- *Classification of Information* – Audit Report No.7, 1999–2000;
- *Security Clearances* – Audit Report No.22, 2001–2002;
- *Physical Security* – Audit Report No.23, 2002–2003; and
- *Management of Protective Security* – Audit Report No.55, 2003–2004.

1.5 Among the key issues arising from these earlier protective security audits are that:

- robust planning processes, preferably integrated with business planning processes, are important to assist in identifying and formalising the priorities, resource levels and the coordination of protective security activities;
- security risk management processes, involving comprehensive security risk assessments and structured risk treatment implementation and monitoring processes, are a critical part of managing protective security;
- comprehensive strategies should be developed to manage security education and training issues and facilitate the measurement and maintenance of security awareness levels;
- the performance of protective security activities, including the effectiveness of the security environment and controls, should be regularly monitored;
- information support systems providing timely, accurate and consolidated management information are important to effectively support protective security activities, in particular, the protection of classified information, the maintenance of security clearances and the accuracy of security-assessed positions; and
- effective security arrangements require a high level of interest and attention from senior management (for example, in the form of a Security Committee). To provide support in this role, management require timely and constructive reports, including information on security performance.

Security incidents and investigations

1.6 A security incident is any activity or occurrence that compromises or has the potential to compromise official resources.⁶ Official information; people who work for, or with the Australian Government; and assets belonging to, or in the possession of the Australian Government; are all included in the definition of official resources. In this regard, the administration of security incidents falls across the above components of protective security, rather than being part of any one particular element.

1.7 Security investigations are a formal tool used to assess the implications of a security incident and in particular, establish the cause and extent of the incident, and identify the appropriate remedial action to prevent further incidents occurring.⁷

1.8 The effective administration of security incidents and investigations is a fundamental part of good security management. Information gathered on security incidents and investigations may highlight the need for entities to re-assess the adequacy of current security practices or arrangements, and can also be a key input into continuous improvement activities.

Protective Security Manual

1.9 The Protective Security Manual (PSM), issued by the Attorney-General, is the principal source of protective security policies, principles and standards for Australian Government entities. Part G of the PSM contains instructions and guidance on the administration of security incidents and investigations. In particular, Part G covers:

- identifying, addressing and recording security incidents;
- analysing incident information to, for example, identify areas of risk, or areas requiring additional security awareness training;
- maintaining staff awareness of the Australian Government's expectations in relation to security incident reporting;
- including information about security incidents in reports to management; and
- the procedures for conducting effective security investigations.

⁶ Attorney-General's Department (2000), *Commonwealth Protective Security Manual 2000*, Canberra, Part G, p. 5.

⁷ *ibid.*, Glossary.

1.10 The Attorney-General's Department is currently finalising a revision of the existing PSM and anticipates that the new Manual will be available in May 2005.

Audit objective and criteria

Audit objective

1.11 The objective of the audit was to evaluate the policies and practices of selected Australian Government entities to determine whether they had established robust arrangements for, and maintained effective control over, the administration of security incidents and investigations.⁸

Audit criteria

1.12 The performance of each entity was assessed against a set of desirable controls or better practice principles (hereafter described as the audit criteria). The audit criteria, which were developed by the ANAO, reflect the requirements and guidelines of the PSM and are reproduced in Appendix 1 of this report.

Audit coverage

1.13 The following entities participated in the audit:

- Australian Crime Commission;
- Australian Customs Service;
- Australian Maritime Safety Authority;
- Child Support Agency; and
- Department of Finance and Administration.⁹

1.14 The audit methodology involved interviews with selected officers, observation and review of policy and procedural documentation, and inspection and examination of documentation relating to a sample of security incidents and investigations.

⁸ The audit focused on non-IT security incidents and investigations. IT security incident handling and reporting processes are being addressed as part of a cross-agency IT security audit expected to be tabled in June 2005.

⁹ The matters discussed in this report are based on the results of the fieldwork undertaken in these entities. However, in accordance with the established practice for protective security audits, this report does not attribute the audit findings to individual entities.

1.15 Each of these entities were provided with a management report detailing the audit findings, recommendations for improvement (where necessary) and conclusions arising from the fieldwork specific to them.

1.16 The audit was undertaken in accordance with the ANAO's Auditing Standards and was completed at a cost of \$215 000.

Structure of the report

1.17 Chapters 2 and 3 outline the findings against each of the audit criteria and also contain recommendations for improving processes around the administration of security incidents and investigations.

2. Management Framework

This chapter discusses the audit findings, including sound and better practices identified in the entities audited, in relation to the framework for the effective management and control of security incidents and the conduct of security investigations.

Introduction

2.1 A robust management framework is essential for the effective administration of security incidents and the conduct of security investigations.

2.2 The elements of the management framework against which the audited entities were assessed are shown in Table 2.1.

Table 2.1

Audit criteria

	Audit Criteria
Policy and procedures	Guidance or reference material is readily available to support the administration of security incidents, including the conduct of security investigations. Roles and responsibilities associated with the management and administration of security incidents (and investigations) are well defined and are understood.
Training and awareness	Relevant staff have received training in relation to security incidents, including investigations. Programs are in place to promote and reinforce awareness about security incidents.
Monitoring and reporting security incident and investigation information	Security incidents (and the results of investigations) are regularly monitored and analysed in order to inform security management processes. Details of security incidents and investigations are regularly communicated to, and acted upon by, management.

Source: ANAO

Policy and procedures

2.3 Current and comprehensive policy and procedural documentation, detailing the approach to the recording, reporting and investigation of security incidents and the associated roles and responsibilities of staff, is important for the effective administration of security incidents and the conduct of security investigations. The nature and content of policy and procedural documentation should reflect the approach taken by the entity to the

management of security incidents and their investigation; the nature of the entity's work; the risks it is exposed to; and the nature and significance of security incidents that have occurred.

Completeness of policies and procedures

2.4 The ANAO assessed the adequacy of relevant policy and procedural documents against the guidelines provided in Part G of the PSM, and sound practice principles. It was expected that policy and procedural documentation would contain information such as:

- a definition of a security incident and the types of incidents likely to be encountered;
- the expected level and nature of response to each type of security incident;
- the processes to report security incidents (both internally and externally);
- the importance of documenting security incidents for future reference;
- the need to assess security incidents to identify any implications and the appropriate level of follow-up action; and
- the need to adhere to relevant legislation, for example, the *Privacy Act*, when dealing with security incidents.

2.5 The ANAO found that, generally, each entity's policies and procedures contained adequate information relating to security incidents and investigations. However, the ANAO also identified that the inclusion of the following matters would improve existing policies and procedures:

- clearly defining a security incident and providing examples of the common types of security incidents that could occur. These measures can assist staff to readily identify when a security incident has occurred and, in turn, facilitate the reporting of security incidents;
- specifying internal reporting requirements and also providing guidance on when security incidents should be reported to the Australian Federal Police (AFP) or other Government agencies, including procedures for reporting details of security incidents and contacts¹⁰ to

¹⁰ An unsolicited encounter with people or organisations that may be an attempt to obtain security or official information they do not have a need to know. *Draft PSM 2005*, Canberra, Part G, p. 5.

the Australian Security Intelligence Organisation (ASIO), and computer security incidents to the Defence Signals Directorate (DSD)¹¹; and

- providing guidance on required actions and outcomes for security investigations, as distinct from other types of investigations. Making a distinction between security investigations and other types of investigations is important because the aim of a security investigation can differ to the aims of other investigations, particularly fraud investigations. The aim of a security investigation is to prevent the incident from re-occurring by making improvements to systems or procedures. It is not necessarily the purpose to establish guilt and aid the prosecution of an offender, as may be the case in a fraud investigation. Part G of the PSM suggests that procedural documentation clearly distinguish between security investigations, and investigations into non-security related incidents.

Currency of policy and procedures

2.6 Policy and procedural documentation should be reviewed on a regular basis to ensure that it remains accurate, and continues to meet the needs of the entity. One way to facilitate timely reviews, is for each document to have a nominated 'owner'; include information on the responsibilities of the 'owner' of the document; and contain information on how staff can contribute to the process of maintaining the currency of the document.

2.7 The ANAO identified that not all the entities audited had formal processes to maintain the currency of their security policy and procedural documentation. As a result, relevant documents did not always reflect current practices, and procedures were not always subject to periodic review. At the time of the audit, each of the entities advised they were in the process of reviewing and updating relevant policy and procedural documents.

Operational roles and responsibilities

2.8 Operational roles and responsibilities associated with the administration of security incidents and the conduct of security investigations should be clearly defined in procedural documentation. The clear definition of roles and responsibilities is particularly important for entities that have adopted a decentralised approach to the administration of security incidents and for the conduct of security investigations, to inform staff of their responsibilities and to promote consistent and uniform processes across the entity.

¹¹ Under the Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS), in cases of, amongst others, loss/theft of laptops.

2.9 Overall, the ANAO found that key roles and responsibilities associated with the administration of security incidents and the conduct of security investigations were generally well understood. However, responsibilities were not always well defined, including in relevant procedural documentation. For example, in one entity, security staff at state offices were expected to play a role in the administration of security incidents but their roles and responsibilities were not clearly defined.

Recommendation No.1

2.10 The ANAO recommends that documentation relating to the administration of security incidents and the conduct of security investigations should, at a minimum:

- specify the roles and responsibilities of staff involved in the administration of security incidents and the conduct of security investigations; and
- include the following information:
 - a definition of a security incident and the types of security incidents common to the entity;
 - guidance on reporting security incidents internally and to relevant external parties;
 - guidance for investigating security incidents, including, distinguishing between the actions required for security investigations and investigations into matters not related to security; and
 - a nominated ‘owner’ and their responsibilities, and the processes for maintaining the currency of the documents.

Entities’ responses

2.11 Each of the entities agreed with the recommendation. Specific comments against the recommendation were provided by the following entities.

Australian Customs Service

2.12 Agreed.

Australian Maritime Safety Authority

2.13 Agreed. The types of security incidents should be provided as guidance only and the processes for maintaining the currency of the documents should be as part of the organisation’s quality management system.

Child Support Agency

2.14 CSA agrees with this recommendation, and advises that it is in the process of expanding its documentation on the administration and conduct of security incidents to include all of the information in the recommendation.

Department of Finance and Administration

2.15 Agreed. Finance has a Security Handbook and Chief Executive Instructions (CEIs) on recording, reporting and managing security incidents.

Training and awareness

Training of security staff

2.16 To assist security staff to discharge effectively their functions, they should be afforded the opportunity to access specialist training. As discussed in Audit Report No.23, 2002–03, *Physical Security Arrangements in Commonwealth Agencies*¹², security works effectively when everyone involved is aware of their responsibilities, and consistently applies the identified controls. Entities should assess the nature and level of involvement of their staff in security functions to determine what training is relevant to each staff member.

2.17 The ANAO assessed that the level of training and experience of staff involved in the administration of security incidents and the conduct of security investigations was appropriate to their functions in each of the entities audited.

Security awareness activities

2.18 In its protective security audit reports, the ANAO has consistently emphasised the importance of an effective program of security awareness activities to support the establishment and maintenance of a strong security culture. A high level of security awareness amongst staff has a number of advantages, including the minimisation of security risks through the consistent application of security controls.

2.19 The key information that should be communicated as part of the promotion of security awareness is identified in Table 2.2.

¹² Australian National Audit Office (2003), *Physical Security Arrangements in Commonwealth Agencies*, Audit Report No. 23, 2002-03, Canberra, p. 48.

Table 2.2**Key security awareness information**

Key security awareness information
Why security is an integral component of the entity's work and supports the entity achieve its goals and mission.
Knowledge of security-related risks and threat sources.
Knowledge of the protective security measures (systems, policies, and procedures) in place, including the security incident reporting/recording mechanisms and requirements.
Details of each staff members' obligations and personal responsibilities in relation to security.

Source: ANAO

2.20 The inclusion of this information in security awareness activities is important to reinforce awareness of security incidents and facilitate the reporting of security incidents. One of the entities involved in the audit experienced a significant increase in reported security incidents as a result of an increase in the level of security awareness, particularly the importance of reporting security incidents.

2.21 The ANAO found that the audited entities used a variety of activities to promote security awareness among their staff. Amongst the sound and better practices observed during this audit were:

- staff being assessed against a range of security awareness competencies, including demonstrating an awareness and understanding of personal security obligations, as part of the performance assessment process;
- an on-line learning package, with tailored modules depending on the security level of staff;
- security awareness emails/fact sheets and security-related alerts being periodically issued to all staff;
- presentations on security awareness being provided regularly;
- individually tailored and targeted security awareness briefings that reflected the entity's environment and risks areas;
- the distribution to all staff of a brochure covering all elements of security; and
- the provision of security kits to managers that contained information, such as:
 - responsibilities in relation to security;

- the entity’s security principles; and
- reporting suspected fraud and security incidents (including police contact procedures).

2.22 Whilst the audited entities had a number of sound and better practice activities in place to promote and reinforce security awareness, none had developed a formal plan or strategy to guide the delivery of security awareness activities, including, where relevant, linkages to business continuity and risk management plans.

2.23 As reported in Audit Report No.55, 2003–04, *Management of Protective Security*,¹³ the ANAO considers that a formal strategy to guide the development and delivery of security awareness activities can facilitate a more coordinated and proactive program of security awareness activities. A structured and planned strategy is also more likely to contribute to better security awareness outcomes in the longer term. Such a strategy could usefully include:

- key objectives of security awareness activities;
- strategies for, and methods of, delivering awareness information and messages, including timeframes;
- identification of the targeted audience, including key external stakeholders;
- appropriate measures of success; and
- the means of monitoring the effectiveness of security awareness activities.

Recommendation No.2

2.24 The ANAO recommends that entities develop a formal plan or strategy for the management and delivery of their security awareness activities.

Entities’ responses

2.25 Each of the entities agreed with the recommendation. Specific comments against the recommendation were provided by the following entities.

Australian Customs Service

2.26 Agreed.

¹³ Australian National Audit Office (2004), op. cit., pp. 32–33.

Australian Maritime Safety Authority

2.27 Agree. For the Authority this is done as part of the Security Plan and monitored via the Security Committee and regular risk review program.

Child Support Agency

2.28 CSA agrees with this recommendation, and advises that it has a formal strategy for the management and delivery of security awareness awaiting approval.

Department of Finance and Administration

2.29 Agreed. Regular security awareness training is provided to all staff on induction.

Monitoring and reporting security incident and investigation information

Monitoring security incident and investigation information

2.30 The regular monitoring and review of security incident records and the outcomes of investigations can be a key element of an entity's continuous improvement process. Regular monitoring can facilitate the prompt identification of potential security weaknesses or threats and assist in the timely implementation of remedial treatments.

2.31 The ANAO observed a number of examples where the audited entities had used information on security incidents and the results of security investigations to improve the effectiveness of security policies and controls, including:

- reassessing the appropriateness of existing controls and identifying the need for further controls;
- reassessing previously identified risks during an update of the Security Plan;
- re-directing investment in security training/awareness activities, for instance, through the delivery of personalised training to address risk areas; and
- disseminating information on the key messages or lessons learnt throughout the entity.

2.32 In some entities the most significant security incidents were analysed by the Security Committee, however, only one entity had formal and regular processes in place to examine and analyse security incident records and investigations reports. In this entity, the process was designed to identify any

systemic issues, threats and opportunities to improve procedures or controls. This entity's documentation on the management of security incidents highlighted that incident reports should be regularly evaluated as part of their continuous improvement activities, in particular to assess:

- the implications for operating procedures;
- whether the level of security risk is increasing;
- potential OH&S implications; and
- the need for new policy and procedures.

2.33 The other entities relied on informal monitoring and review processes, often driven by the significance or circumstance of a particular security incident.

Reporting security incident and investigation information to management

2.34 Strong oversight of operational security matters, including regular reporting to management, is crucial to the effective delivery of protective security functions. This can result in more informed and strategically focussed decisions. It is also important to create and maintain awareness of the general security health of the entity, and gain support from management for the implementation of improvements, such as additional procedures and controls.

2.35 The ANAO found that in each of the audited entities, there was a high level of management oversight of security matters. For instance, most entities had a Security Committee with responsibility for the oversight of protective security. These Committees addressed a range of topics, including the implications of significant security incidents, progress in implementing the entity's Security Plan, and the delivery of security awareness training.

2.36 While the ANAO also found that each of the audited entities provided formal security reports to management, most did not incorporate a discussion on the performance of the protective security function, or an analysis of security incident information.

2.37 As observed in Audit Report No.55, 2003–04, *Management of Protective Security*,¹⁴ security-related reporting is likely to be more effective if it addresses security performance issues. In this regard, a key element of management reporting should be an analysis of security incidents, including the identification of trends and potential exposures, threats or impacts on the security health of the entity.

¹⁴ Australian National Audit Office (2004), op. cit., p. 45.

Recommendation No.3

2.38 The ANAO recommends that entities regularly monitor security incident records and investigations reports, and incorporate an analysis of the impact of security incidents in reports to senior management.

Entities' responses

2.39 Each of the entities agreed with the recommendation. Specific comments against the recommendation were provided by the following entities.

Australian Customs Service

2.40 Agreed.

Australian Maritime Safety Authority

2.41 Agreed. The Authority uses its Security Committee to fill this function.

Child Support Agency

2.42 CSA agrees with this recommendation. A quarterly analysis of this type is provided to the CSA Audit Committee.

Department of Finance and Administration

2.43 Agreed.

3. Security Incidents and Investigations

This chapter discusses the audit findings, including any sound and better practices identified in the entities audited, in relation to the recording of security incident details and the conduct of security investigations.

Introduction

3.1 Relevant details of security incidents should be captured and recorded promptly to facilitate the identification of potential security issues and risks and their subsequent treatment. In turn, effective security investigations should establish the cause of an incident; help to ameliorate the consequences; highlight any security weaknesses (either in policies or their implementation); and identify opportunities to minimise the likelihood of recurrence.

3.2 The audit assessed each entity’s arrangements for the recording of security incidents and the conduct of security investigations against the audit criteria shown in Table 3.1.

Table 3.1

Audit criteria

	Audit Criteria
Recording security incidents details	Processes are in place to capture the relevant details of security incidents efficiently, and in a timely manner. Records of security incidents are maintained efficiently and effectively and are readily accessible.
Conduct of security investigations	Security investigations are planned, managed, conducted and reported in accordance with the standards and guidance material contained in the PSM.

Source: ANAO

3.3 As part of the audit, the ANAO collected details on the number, and nature, of security incidents that had occurred and the number of formal security investigations conducted in the audited entities.

Security incidents

3.4 As shown in Table 3.2, the number of security incidents varied considerably between the five audited entities. The number of security incidents in an entity can depend on a range of factors including: the nature of the entity’s work; the level of security awareness amongst staff; the extent and nature of security monitoring activities undertaken; and the procedures in

place for reporting security incidents. As such, the number of incidents recorded is not, in itself, a reflection of the adequacy or otherwise, of an entity's protective security environment.

Table 3.2

Number of security incidents

	Entity 1		Entity 2		Entity 3 ¹⁵		Entity 4		Entity 5	
Financial year	03/04	02/03	03/04	02/03	03/04	02/03	03/04	02/03	03/04	02/03
Security incidents	60	60	303	225	705	776	14	13	227	465

Source: ANAO, based on the records of the audited entities

3.5 The nature of the security incidents that had occurred in each entity also varied widely and can be broadly categorised under 'property', 'information' and 'people' as shown in Table 3.3.

3.6 The nature of security incidents generally reflected each entity's work, and in turn, the risks to which they were exposed. For instance, entities with a higher level of public interaction had a majority of people related incidents, and entities that had higher proportions of classified or sensitive information holdings, had mainly information related security incidents.

Table 3.3

Examples of security incidents in the audited entities

Property	Information	People
Loss/theft of property, including portable and attractive items	Unauthorised access or release of client data	Contacts ¹⁶
Burglaries and vandalism	Inappropriate handling/storage of classified information	Actual, or the threat of, physical assault on staff or clients
Suspicious incidents within the entity's premises by members of the public	Mail tampering	Harassment of the entity's staff (including offensive behaviour by clients)
Suspicious incidents outside the entity's premises by members of the public		
Unauthorised use, misuse or loss of identification and access cards		

Source: ANAO, based on records of the audited entities

¹⁵ The security incidents shown for this entity are for the calendar years 2004 and 2003, rather than for a financial year.

¹⁶ Refer to footnote no. 10.

Recording details of security incidents

3.7 The efficient capture of consistent and timely information is important for the effective administration of security incidents. Having complete and accurate records of security incidents which are readily accessible should facilitate analysis and reporting on the entity's security performance.

Security incident reporting

3.8 The existence of standard and well-understood processes is important to facilitate the complete, consistent and timely recording of relevant security incident data. The ANAO considers that, as a matter of sound practice, an entity's security policies and procedures should include the requirement for all security incidents to be reported in a standard format. In addition, guidance should be available to staff on how incidents should be reported and on the sources of assistance available (for instance, training, counselling or debriefing).

3.9 Part G of the PSM provides guidance on key information that should be recorded for each security incident, including:

- time, date and location of the security incident;
- description of the incident;
- type of official resources involved;
- description of follow-up and/or remedial action;
- whether the event was caused by negligence or a deliberate activity or an action aimed at compromise; and
- an assessment of any consequences.

3.10 The ANAO found that most of the audited entities had established processes, including standard pro-formas, to capture and report security incident details. Generally, these processes were considered to be well designed and facilitated the complete, consistent and timely capture of key information about security incidents.

3.11 However, the ANAO identified some opportunities for improving the reporting of security incidents, including:

- conducting and documenting an assessment of any consequences of security incidents. An assessment of the consequences of security incidents is considered to be important to determine the extent security may have been compromised, and as a basis for implementing timely corrective action, where necessary; and

- designing reporting processes to minimise the number of security incidents classified as 'other'. A high level of incidents classified as 'other' can make any useful analysis of trends difficult.

Security inspections

3.12 A program of random security inspections will improve an entity's capacity to detect security incidents, and with appropriate follow-up activity, can also generate increased awareness amongst staff of the importance of security controls. It is a particularly useful control measure for entities that hold classified and/or sensitive information and data.

3.13 The ANAO found that arrangements were in place for conducting security inspections in most of the entities that had a significant proportion of classified material. In each case, the ANAO concluded that the inspections provided a pro-active means of managing the risk of breaches of information security requirements.

Constraints to the effective implementation of security inspections

3.14 The audit identified that a number of factors could be seen as barriers to the effective implementation of security inspections, including:

- lack of appropriate storage for classified material;
- the need for further education of its staff on information classification and related security requirements;
- low level of staff awareness of its security controls; and
- funding constraints.

3.15 The ANAO considers it is important that staff are provided with an appropriate level of support and adequate resources and training to be able to secure information appropriately. As such, issues relating to adequate storage and staff training and awareness are important considerations that need to be addressed before the implementation of security inspections.

3.16 The ANAO considers that all entities should consider the benefits of adopting security inspections. Some of the matters to take into consideration in developing a cost-effective and well-targeted program are the frequency of inspections, the extent of checking (a sample of work areas might be targeted during each patrol), responsibility for carrying out the checks, and reporting arrangements. It is also important for entities to determine how security breaches by staff are to be managed, including the reporting of sanctions.

Recommendation No.4

3.17 The ANAO recommends that entities consider implementing a program of security inspections, in light of the risks of the loss, or compromise, of their information holdings or other assets.

Entities' responses

3.18 Each of the entities agreed with the recommendation. Specific comments against the recommendation were provided by the following entities.

Australian Customs Service

3.19 Agreed. Customs conducts regular security inspections of its premises.

Australian Maritime Safety Authority

3.20 Agree, with the basis for the final decision being the organisation's judgement as to the value that would be delivered by such a program, given security measures already in place and risk.

Child Support Agency

3.21 CSA agrees with this recommendation. A strategy to address the security of information holdings, including security inspections, is awaiting approval.

Department of Finance and Administration

3.22 Agreed. Regular security patrols and a summary report of identified instances are an established part of Finance practice.

Recording of security incidents

3.23 Once security incident details are recorded, information should be maintained in a format that facilitates the identification and reporting of trends and new and emerging threats and risks. In this regard, maintaining all security incident details in one system provides opportunities for greater efficiency and enhances an entity's ability to consolidate information and generate useful management reports.

3.24 The ANAO found that most of the audited entities maintained processes to record security incidents that were generally appropriate given their particular circumstances and security environment. Excel spreadsheets, for example, were used by entities that had a low number and low level of significance of security incident activity. More formalised systems such as specialised software and Access databases were used in entities that had a higher level of security incidents.

3.25 The ANAO assessed that some entities could improve the recording of security incidents, by:

- storing all security incident details in one system, leading to greater efficiencies in data capture, analysis and reporting; and
- maintaining records of security incidents that are readily accessible by the ASA and other security staff to assist with effective management of security incidents, particularly in decentralised operating environments.

Recommendation No.5

3.26 The ANAO recommends that entities develop appropriate processes for the consistent and timely reporting and recording of security incident details, including an assessment of the consequences of each incident.

Entities' responses

3.27 Each of the entities agreed with the recommendation. Specific comments against the recommendation were provided by the following entities.

Australian Customs Service

3.28 Agreed.

Australian Maritime Safety Authority

3.29 Agree.

Child Support Agency

3.30 CSA agrees with this recommendation, noting that it has appropriate processes in place and CSA will continue to apply and improve them.

Department of Finance and Administration

3.31 Agreed. All security incidents are reported to senior line managers within one working day and to the Executive Board on a monthly basis.

Conduct of security investigations

Introduction

3.32 The number of security incidents that were formally investigated is comparatively low and is shown at Table 3.4.

Table 3.4

Number of formal security investigations

	Entity 1		Entity 2		Entity 3		Entity 4		Entity 5	
Financial year	03/04	02/03	03/04	02/03	03/04	02/03	03/04	02/03	03/04	02/03
Formal security investigations	13	19	5	5	62	61	0	0	18	22

Source: ANAO, based on records of the audited entities

3.33 The audit found that the majority of security incidents related to matters that did not warrant a formal investigation. For example, many security incidents were of a minor, or procedural nature and were dealt with by local managers or supervisors taking remedial action or were addressed through the conduct of routine inquiries.

3.34 Examples of action taken to address security incidents that did not warrant the conduct of formal investigations included:

- providing further guidance to staff on appropriate handling and storage practices for classified information;
- informing the police or ASIO, as appropriate, in the case of burglaries, vandalism, contacts, suspicious behaviour or harassment of staff by members of the public;
- installing additional security and/or controls in response to cases of theft of petty cash or the loss of minor value portable and attractive items; and
- analysing access-logs in an attempt to identify potential suspects in cases of theft of minor value portable and attractive items.

The decision to investigate

3.35 The decision on the most appropriate response to a security incident is an important part of the management of security incidents. An entity's response to each security incident will be influenced by a number of factors, such as the nature and potential consequences of the incident, and the cost and likely benefits of conducting a formal security investigation.

3.36 To assist in determining the most appropriate response in each case, all security incidents should be categorised and/or prioritised according to agreed criteria.

3.37 As discussed above, the audited entities undertook a range of responses, including inquiries, informal investigations and other actions, to address security incidents. In only a small proportion of cases were formal security investigations undertaken.

3.38 Generally, the audit identified that responses by entities in respect of reported security incidents were appropriate. Minor security incidents were generally addressed by less formal mechanisms, such as procedural inquiries, and more serious incidents were the subject of formal investigation. In some cases, preliminary investigations were conducted if, for example, all the details or the extent of the impact of a security incident were not known before deciding whether, or not, to conduct a formal investigation.

3.39 However, most of the entities audited did not have formal processes to categorise or rank security incidents according to their nature or seriousness. One entity did have a system for ranking its security incidents as part of its assessment of the need for a formal investigation, although a formal record of these rankings was not maintained. One entity advised that decisions whether or not to proceed with a security investigation were recorded on the security incident report. In the other entities, the decision as to whether or not an incident should be formally investigated, and who made it, was generally not documented.

3.40 To enhance the transparency and accountability of decisions relating to the conduct of investigations into security incidents, the ANAO considers that responsibility for determining the response to be taken to each security incident should be clearly assigned to individual managers or work areas. The decision to undertake a security investigation, or any other action to address a security incident should be recorded, together with the ranking or priority given to individual investigations. Finally, summary details of the response to each security incident should be included in management reports.

Recommendation No.6

3.41 The ANAO recommends that:

- responsibility for deciding on responses to security incidents be clearly assigned to individual managers or work areas;
- decisions on the response to be taken on each security incident be properly documented; and
- summary details of responses to security incidents be included in management reports.

Entities' responses

3.42 Each of the entities agreed with the recommendation. Specific comments against the recommendation were provided by the following entities.

Australian Customs Service

3.43 Agreed. Regional Security Advisers have the initial responsibility for responding to incidents and report on incidents and responses to their respective Regional Director.

Australian Maritime Safety Authority

3.44 Agree. The responsibility for these decisions should follow functional lines with guidance from security staff. Decisions should be made at a level appropriate to the severity of the incident.

Child Support Agency

3.45 CSA agrees with this recommendation, and is currently improving the application of these processes in CSA's regional sites as part of the Regional Security Manager role being established.

Department of Finance and Administration

3.46 Agreed. Finance's Security Unit records and follows up on security related incidents in consultation with line managers within one working day of occurrence.

Security investigations

3.47 The PSM provides guidance on the conduct of security investigations and refers to a number of phases relevant to security investigations, including:

- setting the parameters of the investigation;
- collecting relevant information and evidence;

- processing the information and evidence; and
- the dissemination of findings and outcomes of the investigation.

3.48 The ANAO tested a sample of security investigations conducted in the last financial year (2003–04) to determine whether these had been conducted in accordance with the guidelines provided in Part G of the PSM. In particular, the ANAO evaluated:

- whether investigations were properly planned, including: the existence of clear and comprehensive statements of the aims and terms of reference; details of resource allocations; timeframes; and the form of final report;
- if comprehensive records were maintained, including evidence of the provision of certain information to the subjects of investigations or people whose interests may be adversely affected;
- if management were briefed on the progress and the outcomes of each investigation;
- whether investigations had been conducted promptly; and
- whether the investigator followed the parameters set for the investigation by management.

3.49 While the ANAO found that security investigations were generally planned, managed and conducted in accordance with the standards and guidance material contained in the PSM, sample testing of documentation relating to security investigations identified that entities did not always maintain complete information about investigations, such as:

- the terms of reference;
- whether people who were the subject of the investigation were informed about their rights and obligations; and
- whether the need for legal advice was considered.

3.50 The ANAO noted that contractors were, at times, engaged to conduct the more significant or sensitive investigations and also that the conduct of security and security-related investigations was often shared between security staff and other work areas, including Internal Audit and investigation units.

3.51 Where investigation functions are shared, mechanisms should be in place for the communication of security-related issues and findings arising from these investigations to security staff so that they can make, as necessary, timely improvements to systems or procedures to prevent the incident from re-occurring.

3.52 The ANAO found a lack of formal or established mechanisms for communicating security-related information between, and amongst, security staff and other work areas involved in security investigations, or investigations with security-related implications. Entities tended to rely on less formal arrangements, including providing oral advice or information to key staff or managers.

Recommendation No.7

3.53 The ANAO recommends that entities establish formal mechanisms for communicating information between security staff and other work areas involved in security or security-related investigations.

Entities' responses

3.54 Each of the entities agreed with the recommendation. Specific comments against the recommendation were provided by the following entities.

Australian Customs Service

3.55 Agreed.

Australian Maritime Safety Authority

3.56 Agree. In small organisations, use of existing alternative forums such as routine meetings and email may be appropriate.

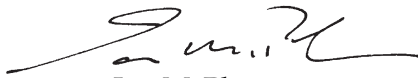
Child Support Agency

3.57 CSA agrees with this recommendation, and is considering options to expand and improve formal communication mechanisms that already exist.

Department of Finance and Administration

3.58 Agreed.

Canberra ACT
15 April 2005



Ian McPhee
Auditor-General

Appendices

Appendix 1: Audit Criteria

Management Framework	
Policy and procedures	<p>Guidance or reference material is readily available to support the administration of security incidents, including the conduct of security investigations.</p> <p>Roles and responsibilities associated with the administration of security incidents (and investigations) are well defined and are understood.</p>
Training and awareness	<p>Relevant staff have received training in relation to security incidents, including investigations.</p> <p>Programs are in place to promote and reinforce awareness about security incidents.</p>
Monitoring and reporting security incident and investigation information	<p>Security incidents (and the results of investigations) are regularly monitored and analysed in order to inform security management processes.</p> <p>Details of security incidents and investigations are regularly communicated to, and acted upon by, management.</p>
Security Incidents and Investigations	
Recording security incidents details	<p>Processes are in place to capture the relevant details of security incidents efficiently, and in a timely manner.</p> <p>Records of security incidents are maintained efficiently and effectively and are readily accessible.</p>
Conduct of investigations	<p>Security investigations are planned, managed, conducted and reported in accordance with the standards and guidance material contained in the PSM.</p>

Appendix 2: Entities' responses to the audit report

This appendix contains the general comments received on the audit report, together with any detailed responses to the recommendations that are not shown in the body of the report.

Australian Crime Commission

The Australian Crime Commission (ACC) agrees with the seven recommendations listed in the audit report. Those recommendations are reflective of both the letter and spirit of the Commonwealth protective security policy as outlined in Part G of the Commonwealth Protective Security Manual 2000 (PSM). The ACC is in the process of updating its Security Policy and Procedures in relation to security incidents and investigations, revising its agency Security Plan and initiating a number of security projects and activities in 2005 which will address, in both broad and specific terms, all of these seven recommendations.

The ACC is pleased that the audit identified a number of areas where the ACC demonstrated sound practices in relation to the administration of security incidents and also identified that, at the time of the audit, the ACC's Security Risk Management Plan 2004–2007 included a number of initiatives that should address some of the key audit findings.

Australian Customs Service

The responses provided by the Australian Customs Service are shown after the recommendations in the body of the report.

Australian Maritime Safety Authority

The responses provided by the Australian Maritime Safety Authority are shown after the recommendations in the body of the report.

Child Support Agency

CSA agrees with the seven recommendations in the Report, and is pleased to note that CSA provided examples of sound and better practice in all four of the areas examined by the ANAO, namely:

- policies and procedures;
- training and awareness;
- monitoring and reporting security incident and investigation information to management; and
- recording security incident details.

Department of Finance and Administration

The responses provided by the Department are shown after the recommendations in the body of the report.

Attorney-General's Department

The Attorney-General's Department agrees with the recommendations contained in the report. The Department regards the ANAO's protective security audits as a valuable tool in the development of Australian Government protective security policy.

Index

A

Audit criteria, 6, 26, 36
Australian Security Intelligence
 Organisation
 ASIO, 6, 28
awareness, 5, 6, 11-12, 14, 16, 21-23,
 26, 30-34, 36, 39, 49-50

D

Defence Signals Directorate
 DSD, 6, 28

M

monitoring, 22, 32-34, 36, 50

P

policies and procedures, 27, 38, 50
Protective Security Manual, PSM, 5, 6,
 11, 23, 50

R

recommendation, 15, 17, 29, 30, 32-33,
 35, 40-41, 44, 46
reporting, 5, 11-12, 14-16, 23-24, 26-
 27, 29-34, 37-41, 49-50
roles and responsibilities, 15, 26, 28-29

S

Security Committee, 22, 33-35
security incident, 3, 5, 7, 11-17, 23-44,
 49-50
security investigation, 5, 7, 12-13, 15,
 23, 26, 28-30, 33, 36, 42-46, 49

T

training, 12, 22-23, 26, 30, 33-34, 38-
 39, 49-50

Series Titles

Audit Report No.40 Performance Audit
The Edge Project

Audit Report No.39 Performance Audit
The Australian Taxation Office's Administration of the Superannuation Contributions Surcharge

Audit Report No.38 Performance Audit
Payments of Good and Services Tax to the States and Territories

Audit Report No.37 Business Support Process Audit
Management of Business Support Service Contracts

Audit Report No.36 Performance Audit
Centrelink's Value Creation Program

Audit Report No.35 Performance Audit
Centrelink's Review and Appeals System

Audit Report No.34 Performance Audit
Centrelink's Complaints Handling System

Audit Report No.33 Performance Audit
Centrelink's Customer Satisfaction Surveys

Audit Report No.32 Performance Audit
Centrelink's Customer Charter and Community Consultation Program

Audit Report No.31 Performance Audit
Centrelink's Customer Feedback Systems—Summary Report

Audit Report No.30 Performance Audit
Regulation of Commonwealth Radiation and Nuclear Activities
Australian Radiation Protection and Nuclear Safety Agency

Audit Report No.29 Performance Audit
The Armidale Class Patrol Boat Project: Project Management
Department of Defence

Audit Report No.28 Performance Audit
Protecting Australians and Staff Overseas
Department of Foreign Affairs and Trade
Australian Trade Commission

Audit Report No.27 Performance Audit
Management of the Conversion to Digital Broadcasting
Australian Broadcasting Corporation
Special Broadcasting Service Corporation

Audit Report No.26 Performance Audit
Measuring the Efficiency and Effectiveness of E-Government

Audit Report No.25 Performance Audit
Army Capability Assurance Processes
Department of Defence

Audit Report No.24 Performance Audit
Integrity of Medicare Enrolment Data
Health Insurance Commission

Audit Report No.23 Performance Audit
Audit Activity Report: July to December 2004
Summary of Results

Audit Report No.22 Performance Audit
Investment of Public Funds

Audit Report No.21 Financial Statement Audit
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2004

Audit Report No.20 Performance Audit
The Australian Taxation Office's Management of the Energy Grants (Credits) Scheme

Audit Report No.19 Performance Audit
Taxpayers' Charter
Australian Taxation Office

Audit Report No.18 Performance Audit
Regulation of Non-prescription Medicinal Products
Department of Health and Ageing
Therapeutic Goods Administration

Audit Report No.17 Performance Audit
The Administration of the National Action Plan for Salinity and Water Quality
Department of Agriculture, Fisheries and Forestry
Department of the Environment and Heritage

Audit Report No.16 Performance Audit
Container Examination Facilities
Australian Customs Service

Audit Report No.15 Performance Audit
Financial Management of Special Appropriations

Audit Report No.14 Performance Audit
Management and Promotion of Citizenship Services
Department of Immigration and Multicultural and Indigenous Affairs

Audit Report No.13 Business Support Process Audit
Superannuation Payments for Independent Contractors working for the Australian Government

Audit Report No.12 Performance Audit
Research Project Management Follow-up audit
Commonwealth Scientific and Industrial Research Organisation (CSIRO)

Audit Report No.11 Performance Audit
Commonwealth Entities' Foreign Exchange Risk Management
Department of Finance and Administration

Audit Report No.10 Business Support Process Audit
The Senate Order for Departmental and Agency Contracts (Calendar Year 2003 Compliance)

Audit Report No.9 Performance Audit
Assistance Provided to Personnel Leaving the ADF
Department of Defence
Department of Veterans' Affairs

Audit Report No.8 Performance Audit
Management of Bilateral Relations with Selected Countries
Department of Foreign Affairs and Trade

Audit Report No.7 Performance Audit
Administration of Taxation Rulings Follow-up Audit
Australian Taxation Office

Audit Report No.6 Performance Audit
Performance Management in the Australian Public Service

Audit Report No.5 Performance Audit
Management of the Standard Defence Supply System Upgrade
Department of Defence

Audit Report No.4 Performance Audit
Management of Customer Debt
Centrelink

Audit Report No.3 Business Support Process Audit
Management of Internal Audit in Commonwealth Organisations

Audit Report No.2 Performance Audit
Onshore Compliance—Visa Overstayers and Non-citizens Working Illegally
Department of Immigration and Multicultural and Indigenous Affairs

Audit Report No.1 Performance Audit
Sale and Leaseback of the Australian Defence College Weston Creek
Department of Defence

Better Practice Guides

Public Sector Audit Committees	Feb 2005
Fraud Control in Australian Government Agencies	Aug 2004
Security and Control Update for SAP R/3	June 2004
AMODEL Illustrative Financial Statements 2004	May 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
Contract Management	Feb 2001
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Managing APS Staff Reductions (in Audit Report No. 49 1998–99)	June 1999
Commonwealth Agency Energy Management	June 1999

Cash Management	Mar 1999
Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	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
Public Sector Travel	Dec 1997
Audit Committees	July 1997
Management of Corporate Sponsorship	Apr 1997
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Asset Management Handbook	June 1996