The Auditor-General
Audit Report No.55 2003–04
Protective Security Audit

Management of Protective Security

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 80785 X

COPYRIGHT INFORMATION

Australian National
Audit Office

Canberra ACT
23 June 2004

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*. I present the report of this audit and the accompanying brochure to the Parliament. The report is titled *Management of Protective Security.*

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

Yours sincerely

P. J. Barrett
Auditor-General

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

AUDITING FOR AUSTRALIA

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

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

John Hawley
Bill Bonney
Ben Matthes

Contents

Abbreviations/Glossary

ANAO	Australian National Audit Office
APS	Australian Public Sector
Evaluation criteria	Normative or desirable controls or processes (that are at reasonable and attainable standards) against which the subject matter under review is assessed.
HRMIS	Human Resource Management Information System
ITT	Information Technology and Telecommunications
Protective security	A broad concept covering information, personnel, physical and information technology and telecommunications security.
PSB	Protective Security Bulletin
PSM	Protective Security Manual
PSCC	Protective Security Coordination Centre
PSPC	Protective Security Policy Committee
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 clearance process	The process of assessing a person's suitability for access to security classified information.
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. Security issues continue to receive widespread attention in the Parliament, the media and amongst the general public. In large part, this attention is fuelled by the continuing volatility of the international security-related environment, in particular, the recurring spectre of, and the continuing threats from, terrorist activity.

2. Given this heightened level of interest, all organisations in the Australian Public Sector need to be able to make informed decisions about, and have the capability to respond to, any potential risks and threats to the security of their assets, including information and their people. In particular, they need to design administrative processes to continually protect their assets from loss, harm or compromise. These processes are collectively referred to as the protective security function.

3. The Protective Security Manual is the main source of protective security policies, principles and standards for Commonwealth organisations. The manual provides guidance and advice on the policies and practices that are important in the development of an effective protective security function.

Audit objective and scope

4. The objective of the audit was to assess whether protective security functions in selected organisations were being effectively managed. In considering effectiveness, the audit assessed whether protective security arrangements:

- were designed within the context of the business framework and the related security risks identified by the organisation; and
- provided an appropriate level of support for the organisation's operations and the delivery of its services.

5. The audit was designed to evaluate the broader management issues associated with protective security, rather than examine the delivery of individual protective security practices. For example, the audit evaluated processes around the development of protective security plans and the management of security-related information. It also considered how each organisation satisfied itself that its security plans and policies continued to be appropriate and were being complied with.

6. The audit did not consider activities associated with the protection of Australia's national security, in particular, counter-terrorism initiatives, which will be reviewed in a forthcoming audit.

Audited organisations

7. The following organisations participated in the audit:

- Australian Taxation Office;
- Commonwealth Scientific and Industrial Research Organisation;
- Department of Family and Community Services; and
- Special Broadcasting Service Corporation.

Audit conclusion

8. Overall, the ANAO concluded that not all the audited organisations had, at the time of the audit, sufficient and reliable processes in place for the effective management of their protective security functions. In particular, while the ANAO observed a positive trend towards greater senior management involvement and commitment in relation to protective security issues, we noted that the effectiveness of some practices was, at times, adversely impacted by resourcing difficulties and the lack of formal oversight and control.

9. The ANAO also considered that some of the organisations were too reliant on processes that were largely undertaken in isolation, or were reactive in nature, rather than being designed as part of a coordinated response to the business and security risks faced.

10. At the time of the audit, there were several significant reforms in progress amongst the audited organisations. The implementation of these reforms is expected to address many of the shortcomings identified by the ANAO.

11. The ANAO also identified a number of opportunities, including those matters being addressed at the time of the audit, to improve the management of protective security functions. These mainly related to:

- the need for better security planning—including the integration of security planning with business planning processes, and the adoption of processes for managing progress against those plans;
- better management of security risks—by integrating security risk management processes with organisation-wide risk management arrangements; and/or by adopting formal and structured processes over implementation and monitoring of risk treatment activities;
- developing strategic, whole-of-organisation approaches to the management of security education and training, and the maintenance of security awareness levels; and

- the need for greater investment in processes for the documentation and monitoring of, and the reporting on, the performance of protective security activities and arrangements.

Sound and better practices

12. The following tables highlight examples of the sound and better practices observed amongst the audited organisations.

Table 1

Sound and better practices in relation to the protective security environment

Protective security environment
Two organisations had established security committees to oversee the management of protective security activities.
Two organisations were, at the time of the audit, developing formal strategies to set the priorities and direction for the delivery of security awareness education and training activities.

Source: ANAO, based on audited organisations' information

Table 2

Sound and better practices in relation to security risk management

Security risk management
In one organisation, the management of security risks occurred as an integral part of the approved organisation-wide risk management processes.
One organisation was preparing, at the time of the audit, a comprehensive plan to oversee the management of its security risks, including the conduct of security-risk assessments and the monitoring of risk treatment strategies and activities.
One organisation had established formal processes for routinely seeking independent information on its potential external threat environment.

Source: ANAO, based on audited organisations' information

Table 3

Sound and better practices in relation to information, monitoring and review

Information, monitoring and review
Three of the organisations had implemented databases to improve the effectiveness of their management of security clearance processes, including their capacity to identify those security clearances requiring review. One of these organisations proposed to interface the database to its Human Resource Management Information System to further assist in maintaining the accuracy and currency of security-clearance records.
One of the organisations routinely captured and reported information on its security-related performance to its senior management.

Source: ANAO, based on audited organisations' information

Recommendations

13. Based on the experiences of the audited organisations, the ANAO made four recommendations designed to improve the management of protective security functions in all Australian Government organisations.

Responses provided by organisations

14. Each of the audited organisations, together with the Attorney-General's Department,[1] responded positively to the opportunity to comment on the proposed audit report.

15. Each of these organisations indicated that they agree with the recommendations. Organisations' responses to the recommendations are shown following each recommendation in Chapters 2–4. Other general comments provided by these organisations are reproduced at *Appendix 1*.

[1] The Attorney-General's Department was asked to comment on the draft report given its central policy role in relation to protective security.

Recommendations

The following recommendations are based on the findings of the fieldwork at the audited organisations. The ANAO considers that they are likely to be relevant to all organisations in the Australian Public Sector. All organisations should 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. 2.26
Security Planning

To enhance the value of security planning processes in the management of protective security, the ANAO recommends that:

- plans for the delivery of protective security activities be prepared as an integral part of, or are fully informed by, business planning processes;
- planning for the various components of the protective security function be integrated across the organisation as far as possible; and
- progress against the key activities and strategies in these plans be monitored regularly.

Recommendation No.2
Para. 2.46
Security Awareness

To facilitate the achievement of broad and enduring improvements to security culture, the ANAO recommends that organisations develop and implement a structured and proactive security awareness education and training strategy.

Recommendation No.3
Para. 3.22
Security Risk Management

The ANAO recommends that organisations establish structured and robust control and oversight arrangements to better support the management, including documentation of security risks, preferably as part of organisation-wide risk management processes.

Recommendation No.4
Para. 4.20
Monitoring Performance

The ANAO recommends that organisations regularly monitor (and report on) the performance of their protective security activities using a range of measures that are pertinent to the security issues faced.

Audit Findings and Conclusions

1. Introduction

The security focus

1.1 Security issues continue to receive widespread attention in the Parliament, the media and amongst the general public. In large part, this attention is fuelled by the continuing volatility of the international security-related environment, in particular, the recurring spectre of, and the continuing threats from, terrorist activity.

1.2 In response to these threats, the Australian Government has put in place a range of measures to assess, identify and react to any potential impacts to Australia's security. These measures include:[2]

- establishment of the National Counter-Terrorism Committee;
- promulgation of the National Counter-Terrorism Plan and the National Counter-Terrorism Handbook;
- introduction of a range of legislation dealing with counter-terrorism activities and cross-jurisdictional offences;
- supporting improvements in the protection of critical infrastructure assets, including upgrading transport and maritime security practices; and
- launching the National Security Public Information Campaign.

1.3 Although not terrorist-related, there have recently been a number of well-publicised security incidents in Australia, including:

- the graffiti attack on the Sydney Opera House by two 'anti-war' protestors;
- the theft of a number of computers from the offices of Commonwealth organisations;
- the unauthorised release, or leaking, of classified government information from a number of Commonwealth organisations; and
- an intruder jumping from the House of Representative's public gallery onto the floor of the chamber (at Parliament House in Canberra).

1.4 When formulating their security arrangements, organisations in the Australian Public Sector (APS), need to make informed decisions about, and have the capability to respond to, a wide range of potential risks and threats. In

---

[2] The National Security website contains more details on these and other measures; <www.nationalsecurity.gov.au>.

Audit Report No.23, 2002–2003, *Physical Security Arrangements in Commonwealth Agencies*, the ANAO suggested the following:

> Rather than reacting to certain events, agencies should be informed as to their specific exposures, and take a strategic and thorough approach to addressing their identified risks.[3]

1.5 Against this background, organisations will require carefully planned security arrangements, in order to continually protect their assets, including information and their people, from loss, harm or compromise. In this report, these arrangements are collectively referred to as the protective security function.

1.6 In designing their protective security arrangements, unless their risk assessment activities indicate otherwise, organisations also need to understand how these broader security issues, such as a major security event and the Government's counter-terrorism measures, might interact with, or impact on, their business.

Protective security

1.7 The term 'protective security' encompasses the policies and practices used to assist in the protection of resources across the following dimensions:

- physical security (including employees' safety)—including the operation of perimeter and building access controls and duress alarm systems;
- administrative or information security—including the classification of personal and official information, which the unauthorised use or disclosure of, could cause distress, harm or damage;[4]
- personnel security—including the processing of security clearances for staff with access to classified information or areas; and
- information technology and telecommunications (ITT) security—including logical access controls, the protection of software, data storage and transmission and network connectivity issues.

1.8 These elements of protective security need to be subject to strong oversight, control, and coordination, to ensure they are delivered in a consistent and complimentary manner. Weaknesses in one element can impact on the effectiveness of, or compound the risks attached to, another element.

---

[3] Australian National Audit Office, Audit Report No.23, 2002–2003, *Physical Security Arrangements in Commonwealth Agencies*, Canberra, p. 16.

[4] The protection of personal information, pursuant to the requirements of the *Privacy Act 1988*, is an integral part of the protective security function.

For example, the strength and reliability of physical barriers can be counteracted if the suitability of individuals with access to classified or sensitive information is not regularly re-evaluated, or if staff are not vigilant in their approach to the handling and transmission of such information.

Protective security audits by the ANAO

1.9 Following a recommendation from the 1979 Inquiry into Protective Security, undertaken by Mr Justice Hope, the ANAO commenced a program of audits to evaluate protective security arrangements in Commonwealth Government organisations. In the majority of cases, these audits were conducted and reported on an individual organisation basis (that is, independently from each other).

1.10 In 1995, the ANAO included protective security audits in its cross-agency general performance audit program. Since that time, the ANAO has undertaken a number of protective security audits, including the following:

- 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*; and
- Audit Report No.23, 2002–2003, *Physical Security Arrangements in Commonwealth Agencies*.

1.11 These audits have consistently identified shortcomings in some of the broader management issues overlaying the delivery of protective security practices. Most significantly, these audits have reported weaknesses in the level and nature of:

- security-risk management processes;
- security awareness and education programs; and
- formal planning of the protective security function.

Protective Security Manual

1.12 The Protective Security Manual (PSM) is the main source of protective security policies, principles and standards for Commonwealth organisations. The PSM provides guidance and advice on the policies and practices important in the development of an effective protective security function.[5]

Protective Security Coordination Centre

1.13 The Protective Security Coordination Centre (PSCC), a Division in the Attorney General's Department, is responsible for contributing to the maintenance of effective protective security practices, procedures and standards in the Commonwealth. It does this through its management of the PSM, the provision of advice on current security policy and practices, the conduct of information sessions, and the provision of security training.

1.14 From time to time, the Centre also issues Protective Security Bulletins (PSB) to provide clarification or additional information on protective security matters and to highlight emerging protective-security related issues. During 2003 for example, it issued six bulletins covering a variety of security-related issues ranging from, details of Australia's new National Counter-Terrorism Plan, to a series of interpretative statements related to Part C (Information Security) of the PSM.

1.15 On behalf of the Protective Security Policy Committee (PSPC), the PSCC conducts an annual survey of the status of protective security in the Australian Government. This survey is designed to collect data to measure the extent of compliance with the minimum standards contained in the PSM, and to provide a snapshot of the state of protective security in the Australian Government.

1.16 The results of the first annual review, which were presented to the Government in June 2002, were considered in Audit Report No. 23, 2002–2003.[6] The results of the second and third surveys have been combined and are expected to be reported to the Government during June 2004.

1.17 The PSCC's report has identified, amongst the respondent agencies, greater levels of recognition of the importance of security, and a resultant improvement in protective security practices. This general trend towards

---

5 Legal opinion obtained by the Attorney-General's Department indicates that *Commonwealth Authorities and Companies Act 1997* bodies do not have to comply with the PSM unless specifically directed to do so by their Minister. Notwithstanding, the ANAO considers adoption of the measures contained in the PSM, where cost effective, to be good protective security practice.

6 Australian National Audit Office, op. cit., p. 14.

improvement in the management of protective security is consistent with the observations made during this audit.

Audit objectives and focus

1.18 The objective of the audit was to assess whether protective security functions in selected organisations were being effectively managed. In considering effectiveness, the audit assessed whether protective security arrangements:

- were designed within the context of the business framework and the related security risks identified by the organisation; and
- provided an appropriate level of support for the organisation's operations and the delivery of its services.

1.19 The audit was designed to evaluate the broader management issues associated with protective security, rather than examine the delivery of individual protective security practices. For example, the audit evaluated processes around the development of protective security plans and the management of security-related information. It also considered how each organisation satisfied itself that its security plans and policies continued to be appropriate and were being complied with.

1.20 In evaluating the management of protective security, the audit concentrated on processes across three broad dimensions, namely:

- security environment—the protective security function is supported by a formal and coordinated planning and control structure;
- risk management—processes are in place to regularly identify, analyse, assess and monitor security-related risks and threats; and
- information, monitoring and review—information to assist in the management of protective security activities, including the results of performance monitoring, is made available to the right people at the right time.

1.21 Within each of these areas, the ANAO developed, with expert assistance from CIT Solutions Pty Ltd and XTEK Consulting Services Pty Ltd, a series of desirable controls or processes (hereafter described as the evaluation criteria). In developing the evaluation criteria, the ANAO considered the principles for the effective management of protective security contained in the PSM. The evaluation criteria for each of the areas of the audit are outlined in Chapters 2–4 of this report.

1.22 The audit did not consider activities associated with the protection of Australia's national security, in particular, counter-terrorism initiatives, which will be reviewed in a forthcoming audit.

Audit coverage

1.23 The following organisations participated in the audit:

- Australian Taxation Office;
- Commonwealth Scientific and Industrial Research Organisation;
- Department of Family and Community Services; and
- Special Broadcasting Service Corporation.

1.24 These organisations were provided with a management report detailing the audit findings, recommendations for improvement (where necessary), and conclusions arising from the fieldwork specific to them. Each organisation provided comments on their respective report, advising of remedial action taken, or proposed, to address identified weaknesses.[7]

1.25 The audit fieldwork involved interviews with selected officers, the examination of documentation and records supporting the management of protective security and general observations.

1.26 The audit was undertaken in accordance with ANAO Auditing Standards and completed at a cost of approximately $225 000.

Structure of the report

1.27 Chapters 2–4 outline the findings against the ANAO's evaluation criteria and also contain recommendations for improving processes for the management of protective security.

---

[7] While the matters discussed in this report are based on the fieldwork undertaken in these organisations, in accordance with established practice for protective security audits, the report does not attribute the audit findings to individual organisations.

2. Protective Security Environment

Introduction

2.1 Formal and coordinated planning and control processes, including an appropriate level of support from senior management, are key elements in an effective protective security function. Protective security should not be regarded as a peripheral or support function. Organisations will be better prepared to identify and deal with security issues, where the management of security is seamlessly integrated with the organisation's governance and planning processes.

2.2 To support the effective translation of security planning and control processes into day-to-day operations and practices, organisations will require their staff to maintain a strong security focus. This is often described as the security culture, which is defined in the PSM as:

> The ready acceptance by people that the securing of official information and other resources is an important and integral part of everyday work practices.[8]

2.3 In the absence of a strong security culture, related activities and practices are less likely to be properly aligned with the strategies and objectives set out in planning documentation.

2.4 In considering the effectiveness of the protective security environment, the audit assessed each organisation against the evaluation criteria shown in Table 2.1.

Table 2.1

Evaluation criteria

Evaluation criteria	Principle
Management support	Senior management provides an appropriate level of support for, or is actively involved in, the design and implementation of security arrangements.
Security planning	A plan, which is fully informed by security risk assessment work, has been prepared to identify and direct the delivery of protective security strategies, priorities and activities.
Policies and procedures	Policies, guidance, procedural and other documentation, designed to manage the threats identified by protective security risk assessment work, have been developed and effectively promulgated to staff.
Security awareness	Security awareness is regularly promoted throughout the organisation.

Source: ANAO

[8] Attorney-General's Department, *Commonwealth Protective Security Manual 2000*, Canberra, glossary.

Management support

2.5 An important part of effective protective security planning and control is a robust and active management structure. Senior management must take an active role in the administration of security-related activity. Without such support, efforts to embed a security culture can be undermined by perceptions (justified or otherwise) of a lack of priority and commitment.

2.6 Overall, the audit found that arrangements for senior management support and involvement, amongst the audited organisations, were largely sound. In particular, the audit observed that senior management were generally affording protective security matters a greater level of attention. The involvement and support of senior management manifested itself in a number of ways, for example:

- three organisations had formally designated a member of the senior executive as responsible for the management of protective security arrangements;
- two organisations had established security committees that were chaired by senior executive officers; and
- the senior governing body of each of the organisations considered, at least periodically, reports on the state of security arrangements.[9]

Key protective security personnel

2.7 Strong oversight and support for protective security staff is critical to assist in the effective delivery of their tasks or functions. For example, constructive senior management involvement can result in more-informed and strategically focussed decisions. It can also facilitate greater consistency in the performance of the tasks or functions and in the implementation of security policies and processes.

2.8 Three of the audited organisations had formally designated, in approved policy or planning documentation, a member or members of their senior executive with responsibility for the oversight of protective security. This was a relatively recent initiative at two of the organisations. At the time of the audit, they were still to confirm the nature of the responsibilities and the measures to address those responsibilities.

2.9 Closely allied to the benefits of a strong oversight role, is the maintenance of good working relationships between the areas responsible for the various elements of protective security, in particular, between the general and ITT functions.

---

[9] Reporting on security matters is discussed further in Chapter 4.

2.10 In each of the audited organisations, the general protective security function was separated, both physically and hierarchically, from the ITT security function.[10] In addition, arrangements for sharing information and the linking of roles and responsibilities between the two functions were generally informal and largely unstructured. In the main, the two functions tended to come together only as events or circumstances dictated.

2.11 Given the complementary nature of these two functions, the ANAO considers they should interact closely, or be integrated in some credible manner, at least in relation to protective security matters. The ANAO, in its audit of the *Operation of the Classification System for Protecting Sensitive Information*[11] observed that the integration of these two functions should facilitate a more comprehensive and consistent approach to the management of protective security.

Security committees

2.12 The establishment of a security committee, to oversee the management of protective security functions, can be an effective way to facilitate greater control and coordination, including the integration of various security responsibilities. It can also be effective in demonstrating senior management involvement.[12]

2.13 Two of the organisations had established security committees to coordinate the management of their protective security functions. Although in one of these, the role and function of the committee had not been clearly defined at the time of the audit. In the remaining organisations, although they did not have separate security committees, security-related issues were periodically addressed in other forums.

2.14 The ANAO recognises that having a separate security committee, is not always a practicable or cost-effective solution. In certain circumstances, it may be appropriate for existing management groups to assume the responsibilities for the management of protective security. In considering whether an existing committee or group is likely to be an effective tool in the overall management of the protective security function, organisations need to consider the extent of that committee's consideration of security issues and the focus and level of its responsibilities.

---

[10] At the time of the audit, one organisation had approved the relocation of its IT security function into its general protective security team, thereby placing them under the same lines of authority.

[11] Audit Report No. 7, 1999–2000, p. 18.

[12] In Audit Report No. 7, 1999–2000, *Operation of the Classification System for Protecting Sensitive Information*, the ANAO recommended that the management of protective security should be coordinated through a security committee (or similar body), p. 18.

Security planning

2.15 The development, implementation and monitoring of a security plan is a central component in the effective management of protective security. The PSM describes a security plan as a plan of action to address the security risks faced by the organisation.[13] The security plan should set the direction and priorities for the security function, nominate the key roles and responsibilities, identify the resources required and establish targets for progress or performance to be measured against.

2.16 Broadly, the audit considered two types of security-related planning:

- annual (or time-sensitive) business or operational planning—to set out, in the context of the organisations' priorities and objectives, the protective security activities required to be undertaken and the resources necessary; and
- periodic security-risk related planning—providing the framework for the implementation of approved security-risk management strategies and treatments.[14]

Annual (or time-sensitive) security planning

2.17 Three of the audited organisations developed formal plans to assist in the identification and management of the direction of their security functions.[15] Across these three organisations, these plans contained:

- links to the organisation's outputs or priorities;
- details of key activities and tasks to be performed;
- details of milestones and key performance indicators;
- details of resources (dollars and people) required;
- definition of key roles and responsibilities;
- an outline of security-related risks; and
- an outline of the current externally sourced threat assessments.

---

[13] Attorney-General's Department, op. cit., Part B, clause 4.9.

[14] This second aspect of security planning is further addressed under the sub-heading '*Monitoring security risk assessments.*'

[15] At the time of the audit, the remaining organisation had commenced development of a plan for the delivery of its security-related functions.

2.18 With the inclusion of this type of information, security plans are more likely to be relevant in supporting the management of protective security functions.

2.19 Although the content of annual security plans was generally appropriate, the ANAO identified several opportunities to improve the contribution of security planning to the management of protective security. In the main, these improvements related to:

- integrating security planning with business planning processes;
- better integrating the planning processes associated with the different elements of the protective security function; and
- monitoring progress against security plans.

Each of these issues is considered in the following paragraphs.

Integrating security planning with business planning processes

2.20 Security is a critical business driver or enabler and should not be regarded merely as a support function. Security planning should be informed by, and in turn inform, the organisation's business planning processes. The security plans of two of the organisations were prepared as part of their business planning cycle.

2.21 The ANAO considered that the preparation of security plans in conjunction with business planning processes, helped ensure that these plans were developed in an appropriate context. In particular, it helped ensure that the management of security activities; and that priorities and strategies (and the resources needed) were aligned and consistent with the wider priorities and strategies of the organisation.

Better integrating the planning processes of the different elements of protective security

2.22 As previously identified, arrangements for sharing of information and the linking of roles and responsibilities between the general and ITT protective security functions were generally poor. This lack of integration extended to security planning processes. Each of the three organisations that had developed formal security plans, had prepared separate plans for their general and ITT protective security functions. The only visible links between the respective plans were the recognition of joint activities (in one organisation) and a reference, in the general security plan of one organisation, to the separate ITT security plan.

2.23 Better integration at the planning stage would support improved coordination in the management and delivery of the protective security function. The ANAO considers that the preparation of a single security plan is

ultimately the best way to facilitate improved coordination. However, given the diverse range of issues, complexities and risks to be addressed, this may not always be the most effective or appropriate approach in some organisations.

2.24 When the preparation of separate plans, to address the discrete elements of protective security, is deemed an appropriate response, better integration can be achieved by linking the common elements in these plans. In these cases, for example, organisations should produce a broad or overarching security plan, supported by one or more detailed subject-specific sub-plans. Each sub-plan should:

- recognise the links between the various plans, and cross-reference all areas of common interest or activity; and
- clearly state its contribution to the overall plan, including the objectives, goals and priorities.

Monitoring progress against security plans

2.25 None of the organisations had formal and structured processes for monitoring and reporting details of the progress against their security plan(s). The monitoring arrangements employed by the organisations audited tended to be informal, involving, for example, discussions at staff meetings and oral reports to management. In particular, the ANAO observed that the general security plan of one of the organisations was not kept up to date. At the time of the audit, this plan was not considered to accurately reflect the functions performed by the security team. In another organisation, the most recent security plan had not been formally approved, or distributed to responsible managers, at the time of the audit.

Recommendation No.1

Security Planning

2.26 To enhance the value of security planning processes in the management of protective security, the ANAO ***recommends*** that:

- plans for the delivery of protective security activities be prepared as an integral part of, or are fully informed by, business planning processes;
- planning for the various components of the protective security function be integrated across the organisation as far as possible; and
- progress against the key activities and strategies in these plans be monitored regularly.

Organisations' responses

2.27 The audited organisations agreed with the recommendation. Specific comments provided for this recommendation are as follows.

Australian Taxation Office

2.28 The Tax Office agrees with the recommendation. In particular:

- the Tax Office will continue to plan for the delivery of protective security activities as an integral part of our business planning processes, through the work of the Security Committee being fed into our corporate planning processes;
- the Security Committee has directed that planning for the various components of the protective security function be integrated as far as possible. This will be supported by the development of an overarching business plan to integrate the work programs of the three areas responsible for the delivery of protective security services; and
- progress against the key activities and strategies in the overarching plan will be monitored regularly by the Security Committee and reported to the Audit Committee. The relevant Assistant Commissioners will regularly monitor implementation of the sub-plans for which they are responsible and report progress to their respective Executives in accordance with normal governance arrangements.

Department of Family and Community Services (FaCS)

2.29 FaCS accepts this recommendation and considers that it already has processes in place to fully meet it. The full text of FaCS' response is reproduced in *Appendix 1*.

Special Broadcasting Service Corporation (SBS)

2.30 SBS supports an approach that sees protective security as an integral part of business planning. This approach is being developed at SBS.

Security policy and procedures

2.31 The existence of clear policy and related procedural documentation is an important tool to support managers and their staff in the conduct of protective security tasks. Sound policy and procedural documentation can assist staff to understand the organisation's security values, and contribute to staff's ability to meet security standards and obligations. It can also explain how staff should react, if they become aware of inappropriate or suspicious behaviour.

2.32 All of the audited organisations had a range of policy and procedural documentation available to support the delivery of their protective security

functions. Overall, the ANAO considered that the available documentation adequately addressed the security issues and the security risks faced by the respective organisations. Furthermore, the ANAO considered that the policy and procedural documentation was generally useful to support managers and their staff in fulfilling their security-related responsibilities.

Reviewing security policy and procedures

2.33 Policy and procedural material should be re-assessed on a regular basis. This is important to ensure that it continues to meet the needs of the organisation, and remains relevant and appropriate, particularly in the light of evolving security issues and risks. Additionally, policy and procedural material should properly reflect the current Commonwealth protective security framework, in particular, the PSM and any protective security bulletins issued by the PSCC.

2.34 None of the audited organisations had formal processes in place to regularly assess the currency, relevance, and accuracy of their security policies and procedural documentation. In most cases, monitoring arrangements tended to be unstructured. As an example, changes were only made to policy and procedural documentation in reaction to events (internal and external) as they occurred, or based on staff reporting any identified inaccuracies or gaps.

2.35 One organisation had a series of measures to assist it in the maintenance of some of its security-related policies. For example, after a policy is promulgated, comments are actively sought from key stakeholders on its adequacy. In addition, certain policies contained a link to an intranet mailbox, which is regularly monitored for staff feedback.

2.36 Two of the audited organisations had recently approved corporate standards for the promulgation of their policies. It is expected that the transition of security policies to meet these new standards, will provide the opportunity for their continued relevance and accuracy to be evaluated.

Security awareness

2.37 The importance of an effective security awareness program has been a common theme in the ANAO's previous protective security audits. For example, in an earlier protective security audit report, the ANAO observed that the organisations in that audit, lacked clear strategies to effectively address security training and awareness issues.[16]

2.38 To support the establishment and maintenance of a strong security culture, organisations need a program to regularly and consistently promote

---

[16] Australian National Audit Office, ibid., p. 15.

and evaluate security awareness across each of the dimensions of protective security. Maintaining a high level of security awareness amongst staff and contractors is an important tool to minimise security risks. In particular, a security awareness program should:[17]

- support the proper implementation of security policies and controls;
- maximise staff's interest in, and their contribution to, protective security practices;
- reduce resistance to inconvenient security procedures;
- support staff becoming fully aware of their security requirements and respective responsibilities;
- promote an understanding of the need for security; and
- explain the potential implications of a breach of the organisation's security, including the costs of the compromise or loss of assets/information.

2.39 The PSM articulates the importance of maintaining high levels of security awareness and vigilance to support effective security practices. It also provides guidance on measures to be considered in the design of security awareness programs.[18] Another useful source of guidance is PSB No. 03/02, which provides information on additional security awareness measures that might be included in any response to the general security alert concerning the increased terrorist threat in Australia.

Promoting security awareness

2.40 The security staff in each of the audited organisations, routinely or periodically provided security awareness training or information sessions. However, with the exception of the provision of security-related orientation sessions for new staff, security awareness training was largely conducted in isolation from, and was not part of, the approved professional development or learning program in any of the audited organisations.

2.41 In addition to this face-to-face contact, the audited organisations also used a variety of mechanisms to promote security awareness amongst their staff. Among the practices observed during the audit were:

- an on-line security awareness program;

---

[17] This list was based on information contained in CIT Solutions Pty Ltd, *Certificate III–Protective Security, Security Awareness and Information Presentation*, Canberra, Module 5, Lesson 1, p. 8.

[18] For example, the PSM requires that appropriate security awareness courses or briefings must be provided; at least every five years, to all Commonwealth employees with a security clearance at, or above SECRET or HIGHLY PROTECTED levels. (paragraph 8.48, p. D62)

- periodically distributing e-mail alerts covering contemporary security issues;
- providing staff with fact-sheets or checklists, containing tips for sound security practices;
- issuing security bulletins to provide advice on protective security issues or guidance on compliance with security requirements;
- including security-related messages in staff newsletters; and
- displaying posters, to highlight key security-related messages, around the workplace.

2.42 However, these processes often occurred in isolation and failed to provide broad or structural improvement in security awareness levels. The ANAO considers that to effectively embed a strong security culture into their day-to-day operational work practices, organisations require a coordinated, multi-faceted and ongoing program or strategy.

2.43 By adopting a program comprising a mix of strategies, organisations will be better placed to achieve the myriad of objectives critical to fostering and maintaining a sound security culture. Some of the key objectives are shown in Table 2.2.

Table 2.2

Security awareness

Objectives of security awareness
The reasons for protective security practices, including the specific and general security-related threats, and the consequences or implications of a breach of security, are understood and accepted.
Staff are conscious of, and assume a greater level of commitment for, both their personal and the organisation's security.
Staff understand their general responsibilities in relation to protective security measures and know whom to contact in relation to more specific security-related matters.
Staff understand how to respond to different security-related incidents, including an emergency event.
Awareness products are tailored to meet the different needs of staff or work-groups.
Awareness messages are routinely and effectively reinforced.
Being security aware and using good security practices is not seen as a hindrance but as an integral part of the organisation's work and important to support the attainment of goals and objectives.

Source: ANAO (based on CIT Solutions Pty Ltd, *Certificate III—Protective Security, Security Awareness and Information Presentation*, Module 5, Lesson 2).

2.44 Another critical component in an effective awareness program is the existence of ongoing monitoring or feedback processes to enable the effectiveness of security awareness initiatives to be measured. For example, assessments might be made of whether:

- staff understand the key messages;
- there are any gaps in the information provided; and
- there are any changes in awareness levels, attitudes and behaviour across the organisation.

2.45 At the time of the audit, two of the organisations were developing plans to formally set out the direction of their security awareness activities, including information on key objectives, strategies and methods of delivering the awareness messages. These plans also identified key measures of success to be used in monitoring the effectiveness of the security awareness strategy. Also, two of the organisations proposed to evaluate their security awareness strategies through the conduct of staff surveys.

Recommendation No.2

Security Awareness

2.46 To facilitate the achievement of broad and enduring improvements to security culture, the ANAO ***recommends*** that organisations develop and implement a structured and proactive security awareness education and training strategy.

Organisations' responses

2.47 The audited organisations agreed with the recommendation. Specific comments provided for this recommendation are as follows.

Australian Taxation Office

2.48 The Tax Office agrees with the recommendation. An integrated and coordinated agency-wide Security Awareness Strategy and Implementation Plan have been endorsed by the Security Committee.

Department of Family and Community Services (FaCS)

2.49 FaCS accepts this recommendation and considers that it already has processes in place to fully meet it. The full text of FaCS' response is reproduced in *Appendix 1*.

Special Broadcasting Service Corporation (SBS)

2.50 SBS presently conducts limited security awareness training and is planning to broaden its current program.

Conclusion—protective security environment

2.51 Overall, the ANAO concluded that the planning and control processes amongst the audited organisations were generally sound. In particular, the audit observed a positive trend towards greater involvement, in protective security matters, by senior management. The ANAO also concluded that, for most of the organisations, policy and procedural documentation was appropriate to support the management and delivery of protective security functions.

2.52 Nevertheless, the audit identified a number of opportunities to strengthen the environment or framework supporting the management of protective security. Most significantly improvements can be made by:

- adopting more robust security planning processes, including integrating security planning into business planning processes and adopting processes for managing progress against the key strategies and activities identified in those plans;
- implementing processes to achieve more-active maintenance of security policy and procedures; and
- developing more strategic and structured programs to deliver and maintain security awareness levels amongst staff and other relevant stakeholders.

3. Security Risk Management

Introduction

3.1 The PSM sets out the principles for, and describes the critical elements in, the management of security-related risks.[19] In summary, the PSM requires organisations to regularly identify, analyse, assess, prioritise, treat and monitor those security risks that pose a threat to the achievement of their objectives. A robust security-risk management process enables organisations to design and maintain security-related controls and activities that are better informed by, and more likely to be effective in, addressing potential threats.

3.2 In an earlier protective security audit report, the ANAO observed that organisations should establish a control framework for the management of its protective security arrangements based on its business and security risks. In particular, that report recommended the following:

> Agencies conduct comprehensive protective security risk assessments, at least every three years as part of an agency-wide approach to risk management and that agencies assess and link the findings arising from ad-hoc periodic security reviews and threat assessments, to the formal security risk assessment.[20]

3.3 The increased profile afforded to security issues and the constantly evolving security environment, places additional onus on organisations to maintain robust security risk management practices. If appropriate security risk management processes are not maintained, organisations may not only fail to recognise or predict potential threats to their operations, but also planned responses may be poorly matched to, and therefore less effective in dealing with, actual risk events.[21]

3.4 In assessing the value of security risk management processes, the ANAO assessed the organisations in the audit against the evaluation criteria shown in Table 3.1.

---

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

[20] Australian National Audit Office, Audit Report No. 23, 2002–2003, *Physical Security Arrangements in Commonwealth Agencies*, Canberra, p. 21.

[21] Security Oz, *Managing the Risks: Securing overseas business operations*, Australian Media Group, Victoria, March/April 2004, p. 82.

Table 3.1

Evaluation criteria

Evaluation criteria	Principle
Security risk assessments	Security-related risk assessments, which are an integral part of, or are fully informed by, organisation-wide planning work and risk assessment activity, are regularly undertaken.
Monitoring risk treatments and controls	There is a systematic and coordinated program in-place for the ongoing management of security-related risk assessments, including the monitoring of risk treatments and controls.

Source: ANAO

3.5 The conduct of security risk assessments and the subsequent monitoring of risk treatments and controls are closely related, and should be seen as part of the same continuum. However, for the purposes of this report, the issues and findings are discussed separately.

Security-risk assessments

3.6 An organisation will not be able to establish and maintain effective protective security controls if it is not fully informed about its security-risk profile. Security risk assessments should not be conducted in isolation, but performed against the context of the organisation's business, and based on an understanding of the organisation's objectives and critical functions. In addition, security-risk assessment work should be properly informed about other planning and risk management activities in the organisation.

3.7 Each of the audited organisations periodically sought information on potential external threats; this included intelligence (written and oral) obtained through the local police forces. Only one of the organisations had established formal processes to routinely obtain a range of intelligence from external organisations.

3.8 Three of the organisations had undertaken comprehensive, organisation-wide reviews to identify and assess their security-related risks. The fourth organisation utilised a rolling program to assess if selected controls and processes were sufficient to address known and potential threats and risks.

3.9 However, at the time of the audit, the ANAO considered that only one organisation had an up-to-date schedule of its security risks. The other organisations had not maintained the currency of their security-risk assessments, or regularly undertaken new assessments.

3.10 In between the conduct of formal reviews, the organisations had tended to rely on one-off and less structured processes to identify new and emerging security risks. This has included, for example:

- staff feedback;
- reviewing security incident reports;
- ad-hoc assurance activities and inspections;
- analysing the results of after-hour inspections; and
- their own general business knowledge.

3.11 The ANAO considers that conducting security risk assessments in isolation, in particular, the failure to integrate or link them to organisation-wide planning or risk management activity, is one of the major reasons that these security risk assessments were not kept up to date. Only one organisation had incorporated the assessment of its security risks into its organisation-wide risk management activity. This matter is further discussed later in this Chapter.

3.12 At the time of the audit, two organisations were developing proposals for the conduct of new organisation-wide security risk assessments. Significantly, both proposals identified how the proposed work supports higher-level corporate priorities. One of the proposals also identified a range of potentially useful information sources. The ANAO considers this is likely to assist the risk assessment being undertaken in the correct context. Relevant potential information sources include:

- security policies and procedures;
- corporate plan, business plans and annual reports;
- fraud control and business continuity plans;
- relevant legislation; and
- other risk management activities.

Monitoring security-risk assessments

3.13 The effective management of security risks requires a systematic and organisation-wide program to document and monitor the assessed risks and related risk-treatment strategies and controls. Documentation is essential for effective risk management, particularly where there are frequent staff changes. Monitoring is important, to identify whether the approved treatment plans are being properly implemented, and to assess whether they continue to be effective. Organisations should also address whether risk treatment strategies remain focused on the areas of greatest risks or exposure, particularly, in light of changes in circumstances and the possible emergence of new risk factors.

3.14 Three of the audited organisations had developed comprehensive plans to assist in the management of their security risks. These plans set out, amongst other things, arrangements for monitoring security risk assessments

and the implementation of the related risk treatments. However, two of these organisations had not kept these plans up to date. As a result, the ANAO considers that these plans no longer made any positive contribution to the management of the security risks. At the time of the audit, these two organisations were finalising proposals to update their security-risk management plans.

Supporting effective monitoring

3.15 A number of factors contributed to these plans not being kept up to date. For example, security issues did not continue to receive sufficient priority, particularly when the organisation went through change. Another reason was that the security staff did not always have sufficient or appropriate authority, to support the implementation and monitoring of organisation-wide risk treatments.

3.16 The ANAO considers that organisations should provide sufficient and appropriate priority and commitment to support the effective monitoring of security risk assessments and the associated treatment plans. One way to achieve this is to incorporate the management of security risks into the organisation-wide risk management program. As identified at paragraph 3.11, only one organisation had incorporated the assessment and management of its security risks with its organisation-wide risk management plan.

3.17 In this case, the assessment of security risks and the associated treatment plans were embedded into the organisation's risk management priorities, and were subject to the same controls and governance arrangements as the rest of the organisation's business risks. This included an annual re-assessment (and report to the Audit and Finance Committee) of the risk events, the relevant controls and, where applicable, their treatment plans.

3.18 A strong framework around the implementation, monitoring and evaluation of security risks treatments, including the identification of new and changing risks, is critical. As observed in this audit, in the absence of a formal and structured framework, processes to monitor the implementation, and to regularly assess the effectiveness (or otherwise), of the risk treatments and controls can be undermined and their effectiveness reduced.

Central coordination and oversight

3.19 A key element in an effective framework is a central coordinating mechanism, with appropriate authority, to oversee all relevant activity. This coordination mechanism might be the Security Committee (or equivalent body). It might be supported, for example, by:

- a program of regular reviews or inspections to assess progress against security risk management plans; and

- regular reporting by responsible managers on progress against plans, including advice as to whether risk treatments remain adequate or appropriate, given for example, any major changes to business objectives or plans.

3.20 Another critical element is a link between the risk treatment plan and security business planning activities. Two organisations considered risks in their security planning process. In particular, the security-business plan of one of these organisations, included a number of references to the implementation and management of the risk treatments identified by security risk management activity.

3.21 Incorporating security risk management strategies into security planning processes is one way that organisations can make certain that appropriate focus is placed, and maintained, on security risk management work. It also facilitates appropriate investment in those areas with the greatest need or risk.

Recommendation No.3

Security Risk Management

3.22 The ANAO ***recommends*** that organisations establish structured and robust control and oversight arrangements to better support the management, including documentation of security risks, preferably as part of organisation-wide risk management processes.

Organisations' responses

3.23 The audited organisations agreed with this recommendation. Specific comments are shown below.

Australian Taxation Office

3.24 The Tax Office agrees with the recommendation. A new Security Risk Management Plan (SRMP) is being developed that will include appropriate mechanisms for assurance and reporting of the implementation of security risk treatment strategies. These mechanisms will include periodic reviews and inspections, the results of which will be reported to the Security Committee. High-level corporate risks will be integrated into the Tax Office's strategic risk management processes. Progress against the SRMP implementation plan will be monitored by the Security Committee and reported to the Audit Committee.

Department of Family and Community Services (FaCS)

3.25 FaCS accepts this recommendation and considers that it already has processes in place to fully meet it. The full text of FaCS' response is reproduced in *Appendix 1*.

Special Broadcasting Service Corporation (SBS)

3.26 SBS currently integrates its security-risk management activities.

Conclusion—security risk management

3.27 Each of the organisations had undertaken reviews to identify their security-related risks. However, the ANAO concluded that three of the organisations had not maintained sufficient attention, or allocated adequate resources, to the ongoing management of security risks. As a result, security risk assessments were not up to date and processes for identifying new and emerging risks were largely informal and unstructured. Furthermore, these shortcomings resulted in an inability to properly monitor the implementation and effectiveness of related security-risk treatment plans.

3.28 The ANAO observed, however, that each of these three organisations were, at the time of the audit, implementing initiatives to update their knowledge of security risks and improve their ability to manage these risks in the future.

4. Information, Monitoring and Review

Introduction

4.1 Access to a range of timely and accurate security-related information, including the results of performance monitoring activities, is critical to assist in the effective management of protective security arrangements. It is also an important element in supporting and informing decision-making processes. In turn, regular monitoring of this information, including comparing it against plans and better practices, is a critical part of the management of a strong security function.

4.2 In addition, details of security activity and outcomes should be prominent in the information provided to senior management; in particular, senior management should receive regular assurance about the security performance of the organisation.

4.3 In considering the effectiveness of information management and monitoring processes, the audit assessed each of the organisations in the audit against the evaluation criteria shown in Table 4.1.

Table 4.1

Evaluation criteria

Evaluation criteria	Principle
Information management	Information useful to the management of protective security processes is readily accessible, maintained in a cost-effective manner and is regularly communicated throughout the organisation.
Monitoring and review	Protective security performance is regularly monitored and reported, including evaluating the effectiveness of, and the level of compliance with, approved policies and practices and assessing the performance of staff against their security-related responsibilities.

Source: ANAO

Information management

4.4 All the audited organisations maintained, and had ready access to, an array of information to support the management of their protective security activities. For example, each of the organisations had access to information on the:

- costs of the protective security function;

- number and type of security clearances;
- volume of classified or sensitive information; and
- details of security incidents.

4.5 The audited organisations sourced security-related information from a variety of records, both electronic and manual. Overall, the audit observed a positive trend towards greater use of electronic records. For example, three of the organisations had developed (or acquired) software to support them in the management of their security clearance programs.[22]

4.6 The ANAO considers that the use of automated records or databases to manage the security clearance process represented a significant enhancement to the organisations' protective security-related information handling capabilities. The databases observed in the audited organisations, provided ready access to sufficient and relevant information to assist in the management of security clearances, including the identification of those security clearances due for review.[23]

4.7 During the audit, one of the organisations advised the ANAO that it proposed to interface the database to its Human Resource Management Information System (HRMIS) to further assist in maintaining the accuracy and currency of security-clearance records. For example, the interface will assist in the identification of those positions requiring a security clearance, and also enable the generation of automatic alerts when a security clearance is due for review.

4.8 This is a major improvement on the situation reported in Audit Report No.22, 2001–2002, which identified that one of the factors leading to the significant number of overdue security clearances identified in that audit, was the lack of the ability to monitor and report on the status of security clearances.[24]

Monitoring and review

4.9 The audit examined the processes employed by organisations to monitor the performance of protective security activities. In evaluating processes for monitoring security-related performance, the audit considered processes associated with the monitoring of performance at two levels:

---

[22] An automated solution was not considered cost-effective in the fourth organisation given the small number of security clearances.

[23] The PSM describes two types of security clearance reviews, namely, 're-validations' and 're-evaluations'. The term 'review' used in this report covers both of these processes.

[24] Australian National Audit Office, Audit Report No.22, 2001–2002, *Personnel Security—Management of Security Clearances*, Canberra, p. 50.

- assessing the performance of those staff with protective security responsibilities; and
- monitoring performance, at the whole-of-organisation level, in terms of compliance with security policies and standards, and also against targets or measures of success.

Assessing the performance of security staff

4.10 Each of the audited organisations regularly assessed the performance of those staff with specific protective security responsibilities. As a rule, these assessments occurred both informally, through for example, regular staff meetings and, more formally, through the organisations' performance appraisal processes.

4.11 Most, but not all, of the staff with protective security responsibilities had detailed their respective security-related responsibilities in their individual performance agreements. The inclusion of these details in performance agreements provides greater certainty in relation to the management of protective security roles and responsibility. It is also an effective mechanism for securing accountability over the delivery of protective security tasks and the achievement of protective security objectives.

Monitoring the security-related performance of the organisation

4.12 Audit Report No.7, 1999–2000 recommended that organisations develop a formal security monitoring and review program to analyse areas of security weaknesses, highlight procedural deficiencies and/or identify where the policies and practices require revision.[25]

4.13 None of the audited organisations had formal programs in place to routinely monitor and assess their whole-of-organisation security-related performance, including the level of compliance with security-related policies and standards. With the exception of technical ITT security reviews, only two of the organisations' Internal Audit Sections had examined protective security issues in the last three years. None of the organisations routinely used self-assessment certifications or checklists to gauge performance levels in operational areas.

4.14 The audited organisations had a variety of processes for measuring and monitoring protective security-related performance. However, some of these tended to be unstructured, or ad-hoc in nature. The practices observed during the audit included:

---

[25] Australian National Audit Office, op. cit. p. 20.

- periodic after-hours inspections to monitor compliance with clear desk policies;
- ad-hoc or one-off reviews (two of the organisations had recently undertaken reviews of their physical security arrangements);
- preparation of commentaries or status reports for senior management, including the security committee;
- regular meetings between protective security staff to assess the progress of activities and discuss related performance issues;
- assessing the performance of contracted security service providers; and
- reviewing actual and forecasted expenditure levels against approved budgeted levels.

4.15 The reviews of security arrangements, observed during the audit, were considered to be useful tools for informing opinions on the effectiveness of protective security arrangements. However, such approaches are unlikely to be as effective, over the longer term, as an ongoing or rolling program, to assess the effectiveness of protective security policies and practices. Further, the reviews observed in the audit were largely limited to evaluating physical security arrangements; they did not address, for example, information security practices.

4.16 At the time of the audit, a number of improvements in relation to the level of monitoring and assurance activity were in train in some of the audited organisations. For example, one of the organisations was developing a program to regularly assess (and report on) its physical security practices, including compliance with the requirements of the PSM and relevant internal standards. The Audit Committee at another organisation had tasked the Internal Audit Section with undertaking an annual review of, and the preparation of a report on, the status of the organisation's protective security and fraud arrangements.[26] The ANAO considers that this attention to security arrangements, by the Audit Committee, is better practice.

4.17 As indicated in Chapter 2, senior management in each of the audited organisations, were routinely provided with reports commenting on protective security matters. Most of the reporting on security tended to be activity or issue-based, or was limited to a general commentary on contemporary issues. Security reporting did not, as a rule, include an assessment of performance, rather any assessment of performance had to be inferred from the facts presented.

---

[26] Although at the time of the audit, neither the scope of these audits nor the approach to be used, had been decided.

4.18 Only one organisation routinely captured and reported information specifically targeting the performance of its protective security arrangements. It routinely reported against a series of performance indicators, including security-related measures. It also reported on its conformance with a range of external and internal requirements, including the PSM, the Australian Communications Electronic Security Instruction 33 (in relation to ITT security) and selected security policies.

4.19 The ANAO considers that security-related reporting to senior management would be more effective if it addressed the organisation's protective security performance. In particular, commentaries should be supported by a set of performance measures. Indicators, or measures, of performance can be a useful tool to focus attention on critical areas and related performance. They also facilitate comparisons and analysis against previous performance or against identified targets or standards. The measures used should be pertinent to the organisation's environment and the security issues it faces. The latter might include, for example:

- analysis of security incident and/or breach statistics, including identification of trends and problem areas;
- progress against security plans;
- results of quality control or assurance activity, including compliance with policies;
- details of waivers sought from the minimum standards in the PSM;
- assessment of the costs of the security function against budgets or forecasts;
- analysis of security clearance statistics, including caseloads; and
- assessment of the effectiveness of security awareness activities, including whether these are contributing to improvements in security culture.[27]

Recommendation No.4

Monitoring Performance

4.20 The ANAO ***recommends*** that organisations regularly monitor (and report on) the performance of their protective security activities using a range of measures that are pertinent to the security issues faced.

---

[27] CIT Solutions Pty Ltd, Certificate III—*Protective Security, Introduction to Protective Security*, Module 1, Lesson 4, p. 2.

Organisations' responses

4.21 The audited organisations agreed with the recommendation. Specific comments are shown below.

Australian Taxation Office

4.22 The Tax Office agrees with the recommendation. The Tax Office will continue to capture and report information targeting the performance of its protective security arrangements, and seek to enhance these processes. Reporting will also include commentary of the performance of the protective security function in delivering security-related services to the organisation.

Department of Family and Community Services (FaCS)

4.23 FaCS, in part, meets this recommendation through the processes it currently has in place. FaCS will also take action to explore the viability of introducing further measures to monitor the performance of protective security activities. The full text of FaCS' response is reproduced in *Appendix 1*.

Special Broadcasting Service Corporation (SBS)

4.24 SBS is examining options to increase and broaden the current levels of monitoring and feedback.

Conclusion—information, monitoring and review

4.25 The ANAO concluded that each of the audited organisations had sound arrangements in place for the management of its security-related information. In particular, the audit observed a positive trend towards the greater use of technology in designing relevant information management capabilities.

4.26 Overall, the ANAO concluded that the audited organisations had sound processes for evaluating the performance of those staff with specific protective security responsibilities. However, the ANAO also observed a lack of regular and structured arrangements for monitoring and assessing security-related performance more broadly, for example, at the whole-of-organisation level. This included a lack of processes for assessing compliance with, and the effectiveness of, security policies and arrangements.

4.27 Generally, reporting to senior management, on security matters, did not contain an assessment of the protective security performance of the organisation. Rather, it was limited to general, or issue-based, commentaries because the organisations lacked any formal mechanisms to assess performance.

Canberra ACT
23 June 2004

P. J. Barrett
Auditor-General

Appendices

Appendix 1: Organisations' responses to the proposed audit report

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

Attorney-General's Department

The Attorney-General's Department supports the evaluation criteria and methodology used in the audit. Although the audit was limited to a small number of agencies, its findings are broadly consistent with the results of the Attorney-General's Department's annual surveys of security across all agencies, which are showing steady improvement in the management of security across government.

The Attorney-General's Department supports the recommendations of the report, which are both consistent with government policy and represent best practice. The Commonwealth Protective Security Manual is currently being revised, and will emphasise the importance of integrating security into organisational culture and taking a structured approach to reviewing security risk management.

Department of Family and Community Services (FaCS)

Recommendation 1

Annual business plans prepared by the Protective Security Section include the delivery of protective security activities and are fully informed by the overall departmental planning process. These plans are sufficiently flexible so that they can be adjusted to take into account any significant change in business direction that may occur during the year.

As noted in the footnote 10 of the report, FaCS is the organisation that has approved the relocation of its IT security function into its general protective security team whilst still maintaining a close working relationship with the IT Branch. In addition to this, the Protective Security Section reports to the same SES Officer as the Property Section and is physically located adjacent to this section. These two measures have integrated the various components of protective security within the Department.

FaCS has established an executive security committee, called the Protective Security Policy Committee (PSPC), which is chaired by a senior executive officer. The role of this committee is to oversee and monitor the delivery and implementation of the protective security framework across the Department. The PSPC regularly reports to FaCS' Executive Board, chaired by the Secretary.

The Department's Internal Audit Section has also been asked by FaCS' Audit Committee to monitor and report on progress against key protective security activities and strategies and they have included an annual review of this into their audit program.

FaCS uses the results of the Attorney General's Department's annual protective security survey as a tool to monitor and report on its level of compliance with minimum standards which are directly linked to key activities and strategies. These results are reported directly to the Secretary, the PSPC and Executive Board.

Recommendation 2

At the beginning of this financial year, FaCS appointed a permanent staff awareness and training officer whose role is to develop, implement and maintain a structured and proactive security awareness education and training strategy across the Department.

In January of this year, a formal Protective Security Communication Strategy was approved. The overall purpose of this Strategy is to ensure that staff at all levels within FaCS understand, and are fully conversant with, all their security obligations and requirements. Specific objectives of the Strategy are to:

- ensure all FaCS staff know their protective security responsibilities and obligations;
- emphasise the importance of all staff taking individual responsibility for security;
- foster and maintain a culture of security awareness within FaCS;
- establish a process for the ongoing development, testing and review of security awareness training in FaCS; and
- develop and implement a Protective Security Communication Strategy that meets all external requirements, including those of the Australian National Audit Office (ANAO).

Security awareness education and training strategies identified in the Strategy have already been implemented across the Department.

Recommendation 3

FaCS is taking action to update its security-risk management plan. Although it would be difficult to fully integrate this plan into organisation-wide risk management processes, the plan will be given to the Department's Risk Management Section so that it can be used to inform other risk management activities being undertaken across FaCS.

In addition to this, FaCS has established structured and robust control and oversight arrangements to support the management of security risks. It is proposed that once the security-risk treatment strategies that are identified during the current protective security risk assessment of all FaCS' sites are accepted, they will form the Department's Security Action Plan (SAP). Although the implementation of individual treatment strategies will be the responsibility of individual business areas, the Protective Security Section will drive and monitor the overall implementation of the SAP and will be required to report on this to PSPC each time it meets.

The PSPC may ask any individual manager responsible for the implementation of a security-risk strategy to report directly to that Committee on the status of that strategy and has indicated that it will do so if it appears that strategies are not being implemented in a timely manner.

As previously mentioned, the PSPC reports to the Executive Board and non-compliance with the SAP would certainly be included in this report.

Recommendation 4

The Protective Security Section already provides the PSPC with an analysis of security incident and breach statistics, including identification of trends and problem areas. This analysis is used to direct future activity specifically targeted to reduce similar incidents and breaches occurring again. This Section undertakes other audits, as required, such as the recent audits of access to Cabinet documents and the restricted access drive.

It is already planned for the Protective Security Section to report to the PSPC progress against the SAP, once finalised.

The Protective Security Section also provides the PSPC each time it meets details of all PSM waivers granted and their expiry dates and an analysis of security clearance statistics.

FaCS will explore developing processes to measure results of quality control or assurance activities and an assessment of the effectiveness of security awareness activities. If it is decided that reporting on these would add value to the Department's protective security framework, action will be taken to also report to the PSPC on these matters.

Commonwealth Scientific and Industrial Research Organisation (CSIRO)

Overall, the report is explicit and provides a sound basis for CSIRO to review and perhaps modify the programs in place, and to initiate and test new programs that will enhance the protective security program. It is only by

review from both internal and external professionals that best practice can be achieved.

Special Broadcasting Service Corporation (SBS)

SBS was pleased to be able to take part in this audit. Protective security is taken very seriously by SBS and is seen as a top administrative priority at present. SBS' work to date on protective security has focussed primarily on areas of high risk. The audit has contributed in developing a wider focus and will assist in broadening SBS' planning and implementation strategies.

Index

Series Titles

Audit Report No.54 Performance Audit
Management of the Detention Centre Contracts—Part A
Department of Immigration and Multicultural and Indigenous Affairs

Audit Report No.53 Performance Audit
The Implementation of CrimTrac

Audit Report No.52 Performance Audit
Information Technology in the Department of Veterans' Affairs—Follow-up Audit

Audit Report No.51 Performance Audit
HIH Claims Support Scheme—Governance Arrangements
Department of the Treasury

Audit Report No.50 Performance Audit
Management of Federal Airport Leases

Audit Report No.49 Business Support Process Audit
The Use and Management of HRIS in the Australian Public Service

Audit Report No.48 Performance Audit
The Australian Taxation Office's Management and Use of Annual Investment Income Reports
Australian Taxation Office

Audit Report No.47 Performance Audit
Developing Air Force's Combat Aircrew
Department of Defence

Audit Report No.46 Performance Audit
Client Service in the Family Court of Australia and the Federal Magistrates Court

Audit Report No.45 Performance Audit
Army Individual Readiness Notice Follow-up Audit
Department of Defence

Audit Report No.44 Performance Audit
National Aboriginal Health Strategy Delivery of Housing and Infrastructure to Aboriginal and Torres Strait Islander Communities Follow-up Audit

Audit Report No.43 Performance Audit
Defence Force Preparedness Management Systems
Department of Defence

Audit Report No.42 Business Support Process Audit
Financial Delegations for the Expenditure of Public Monies in FMA Agencies

Audit Report No.41 Performance Audit
Management of Repatriation Health Cards
Department of Veterans' Affairs

Audit Report No.40 Performance Audit
Department of Health and Ageing's Management of the Multipurpose Services Program and the Regional Health Services Program

Audit Report No.39 Performance Audit
Integrity of the Electoral Roll—Follow-up Audit
Australian Electoral Commission

Audit Report No.38 Performance Audit
Corporate Governance in the Australian Broadcasting Corporation—Follow-up Audit

Audit Report No.37 Performance Audit
National Marine Unit
Australian Customs Service

Audit Report No.36 Performance Audit
The Commonwealth's Administration of the Dairy Industry Adjustment Package
Department of Agriculture, Fisheries and Forestry—Australia
Dairy Adjustment Authority

Audit Report No.35 Business Support Process Audit
Compensation Payments and Debt Relief in Special Circumstances

Audit Report No.34 Performance Audit
The Administration of Major Programs
Australian Greenhouse Office

Audit Report No.33 Performance Audit
The Australian Taxation Office's Collection and Management of Activity Statement Information

Audit Report No.32 Performance Audit
'Wedgetail' Airborne Early Warning and Control Aircraft: Project Management
Department of Defence

Audit Report No.31 Business Support Process Audit
The Senate Order for Department and Agency Contracts
(Financial Year 2002–2003 Compliance)

Audit Report No.30 Performance Audit
Quality Internet Services for Government Clients—Monitoring and Evaluation by Government Agencies

Audit Report No.29 Performance Audit
Governance of the National Health and Medical Research Council
National Health and Medical Research Council
Department of Health and Ageing

Audit Report No.28 Audit Activity Report
Audit Activity Report: July to December 2003
Summary of Outcomes

Audit Report No.27 Performance Audit
Management of Internet Portals at the Department of Family and Community Services

Audit Report No.26 Performance Audit
Supporting Managers—Financial Management in the Health Insurance Commission
Health Insurance Commission

Audit Report No.25 Performance Audit
Intellectual Property Policies and Practices in Commonwealth Agencies

Audit Report No.24 Performance Audit
Agency Management of Special Accounts

Audit Report No.23 Performance Audit
The Australian Taxation Office's Management of Aggressive Tax Planning
Australian Taxation Office

Audit Report No.22 Financial Statement Audit
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2003
Summary of Results

Audit Report No.21 Performance Audit
Special Employee Entitlements Scheme for Ansett Group Employees (SEESA)
Department of Employment and Workplace Relations
Department of Transport and Regional Services

Audit Report No.20 Performance Audit
Aid to East Timor
Australian Agency for International Development

Audit Report No.19 Business Support Process Audit
Property Management

Audit Report No.18 Performance Audit
The Australian Taxation Office's Use of AUSTRAC Data Follow-up Audit
Australian Taxation Office

Audit Report No.17 Performance Audit
AQIS Cost-recovery Systems Follow-up Audit
Australian Quarantine and Inspection Service

Audit Report No.16 Performance Audit
Administration of Consular Services Follow-up Audit
Department of Foreign Affairs and Trade

Audit Report No.15 Performance Audit
Administration of Staff Employed Under the Members of Parliament (Staff) Act 1984
Department of Finance and Administration

Audit Report No.14 Performance Audit
Survey of Fraud Control Arrangements in APS Agencies

Audit Report No.13 Performance Audit
ATSIS Law and Justice Program
Aboriginal and Torres Strait Islander Services

Audit Report No.12 Performance Audit
The Administration of Telecommunications Grants
Department of Communications, Information Technology and the Arts
Department of Transport and Regional Services

Audit Report No.11 Performance Audit
Annual Performance Reporting

Audit Report No.10 Performance Audit
Australian Defence Force Recruiting Contract
Department of Defence

Audit Report No.9 Performance Audit
Business Continuity Management and Emergency Management in Centrelink
Centrelink

Audit Report No.8 Performance Audit
Commonwealth Management of the Great Barrier Reef Follow-up Audit
The Great Barrier Reef Marine Park Authority

Audit Report No.7 Business Support Process Audit
Recordkeeping in Large Commonwealth Organisations

Audit Report No.6 Performance Audit
APRA's Prudential Supervision of Superannuation Entities
Australian Prudential Regulation Authority

Audit Report No.5 Business Support Process Audit
The Senate Order for Departmental and Agency Contracts (Autumn 2003)

Audit Report No.4 Performance Audit
Management of the Extension Option Review—Plasma Fractionation Agreement
Department of Health and Ageing

Audit Report No.3 Business Support Process Audit
Management of Risk and Insurance

Audit Report No.2 Audit Activity
Audit Activity Report: January to June 2003
Summary of Outcomes

Audit Report No.1 Performance Audit
Administration of Three Key Components of the Agriculture—Advancing Australia (AAA) Package
Department of Agriculture, Fisheries and Forestry—Australia
Centrelink
Australian Taxation Office

Better Practice Guides

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	Jun 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)	Jun 1999
Commonwealth Agency Energy Management	Jun 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	Jul 1998

Controlling Performance and Outcomes	Dec 1997
Management of Accounts Receivable	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997
Public Sector Travel	Dec 1997
Audit Committees	Jul 1997
Management of Corporate Sponsorship	Apr 1997
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Asset Management Handbook	Jun 1996