Protective Security

ISSN 1036-7632

ISBN 0 64 4 39048 4

Canberra ACT
4 December 1997

Dear Madam President
Dear Mr Speaker

In accordance with the authority contained in the Audit Act 1901, the ANAO has undertaken an audit of protective security arrangements across a number of Commonwealth agencies.

Due to the nature of protective security arrangements, the audit findings have been reported generically. The findings and recommendations contained in this report are not therefore necessarily attributable to any one agency, based as they are on an accumulation of agency experience.

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

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

Contents

Summary

Summary

Protective security in the Commonwealth

1.1 'Protective security' is the protection of information, assets and people from potential threats and dangers, for example, industrial espionage, theft and abuse. It does not generally cover fire, natural disasters and work safety matters.

1.2 Within the Commonwealth each agency is responsible for establishing protective security arrangements commensurate with its operational responsibilities and environment. However, the processes and controls established to afford protection need to be balanced with each agency's responsibilities for accessibility, openness and accountability.

1.3 The Attorney-General's Department is responsible for the development and coordination of protective security policy. The Department issues standards and guidelines in the form of a Commonwealth protective security manual which it is currently reviewing.

1.4 Additional background and contextual information are provided at Appendix 1.

Audit objectives and criteria

1.5 The objectives of the audit were to determine whether the management and administration of Commonwealth protective security arrangements complied with Government policy, standards and guidelines; and to identify, recommend and report better practice in security management.

1.6 The audit did not include computer security and communications security. These are specialised topics which will be subject to separate independent audit coverage.

1.7 The audit covered security management and administration at thirteen agencies as well as the policy role of the Attorney-General's Department.

1.8 The key criteria for assessing agencies' management and administration of security were taken primarily from the current protective security manual and are categorised below in terms of the overall control framework for an organisation:

- *security control environment* - including the allocation of responsibility for security; the adequacy of policy, procedures and instructions; and the relevance and timeliness of staff training and awareness programs;

- *security risk management* - including the adequacy and frequency of risk review and threat assessment processes, and the related plans for treating threats and dangers;

- *security control measures* - including the adequacy of design and operation of information, personnel and physical security arrangements; and

- *security monitoring and reporting processes* - including the relevance, reliability and timeliness of information provided to management on compliance with security policy and procedures.

1.9 Further information relating to the audit objectives, criteria, scope and approach is provided at Appendix 2.

Audit opinion

1.10 The ANAO found that most agencies had established a protective security framework similar to the model recommended in the Commonwealth protective security manual. However, certain protective security arrangements examined by the audit were not operating in accord with the framework in many of the agencies; and, as a result, the potential for breaches of security was sometimes higher than would normally be desirable.

1.11 The ANAO considered that the main reason for the less than optimum performance at many of the agencies related to inadequacies in the security control environment and, in particular, a general lack of staff awareness of security responsibilities and requirements.

1.12 The need for increased awareness was particularly borne out by breakdowns identified during the audit in the security control procedures relating to the protection of classified information. The ANAO concluded that there is a need to raise the profile of security management and awareness across Commonwealth agencies.

1.13 In addition, there has been a need for some time for the Commonwealth protective security manual to be updated as a result of changes in the public sector and security environments over recent years, eg. organisational changes such as outsourcing, and technological changes such as the increasing reliance on information technology systems. A new issue of the manual is planned for early 1998. The new manual should create an ideal opportunity for raising the awareness of protective security and encouraging improvements in security management within Commonwealth agencies.

Audit findings

1.14 The major audit findings, grouped under the audit criteria on which the audit opinion is based, are as follows:

Security control environment

- insufficient allocation of responsibility and accountability for protective security to program level;
- incomplete security policy and procedure manuals; and
- limited security training for staff, including security officers.

Security risk management

- risk reviews not updated for changes in the security environment; and
- lack of formal planning detailing the treatment of identified risks.

Security control measures

- inadequacies in the classification, handling and storage of classified information including incorrect classification of material, no controls over the copying of documents and lack of appropriate storage facilities; and
- incomplete recording of visitors and after hours access by staff.

Security monitoring and reporting processes

- inadequacies in the monitoring of security incidents, and in the review of automated recording systems; and
- inadequate reporting of security matters to executive management.

1.15 The detailed findings and recommendations are set out in Part Two of the Report. A summary of the recommendations is also provided below.

Better practice

1.16 Better practice principles and guidelines have been included at Appendix 3 of this report. The principles and guidelines are largely based on the revised draft of the protective security manual. The ANAO acknowledges the important work of the Attorney-General's Department in this regard.

1.1

Recommendations

1.17 The ANAO recommendations are as follows:

Recommendation 1
- that the Protective Security Policy Committee:

- decide on a charter covering the objectives of the committee, the composition and status of membership, the frequency and records of meetings, the committee's powers and functions, and accountability requirements; and

- act in accordance with the adopted charter.

(paras 2.5 to 2.9 refer)

Recommendation 2
- that agencies review the allocation of responsibility for security with a view to devolving greater responsibility to program and line managers, whilst at the same time maintaining effective coordination through a security coordinator or similarly designated committee.

(paras 2.12 to 2.16 refer)

Recommendation 3

- that agencies:

- customise policy, procedures and guidelines to deal with the assessed risks applicable to their operations; and consolidate the relevant information into a readily accessible form;

- establish security competencies for staff and assess the degree of effectiveness of security training and awareness programs in operation, and;

- arrange regular formal training in protective security, including induction training for new staff, and specialised training, where appropriate; and promote and communicate security awareness through the use of demonstrations and videos, and publications and electronic means.

(paras 2.17 to 2.23 refer)

Recommendation 4
- that agencies without comprehensive and up-to-date security risk assessments and planning:

- undertake security risk reviews and assessments as part of their risk management process, seeking expert assistance as required;

- develop security plans outlining the activities and resources (costs) necessary to address the identified risks; and

- review and update the security risk assessments and plans at set intervals, eg. three yearly, annually, or when circumstances require it, ie. changes in the security environment.

(paras 2.24 to 2.29 refer)

Recommendation 5

- that agencies:

- maintain systems to record key data on all security incidents and promote the use of the systems to staff;

- investigate security incidents as they arise and monitor the causes and consequences of incidents on an ongoing basis; and

- provide reports on the performance of security operations to executive management at set intervals, eg quarterly, monthly.

(paras 2.35 to 2.37 refer)

Audit Findings and Recommendations

Audit Findings and Recommendations

Commonwealth protective security policy and guidance

1.18 The Protective Security Coordination Centre (PSCC) within the Attorney-General's Department develops and promulgates protective security policy for the Commonwealth. In doing so, the PSCC works closely with certain other agencies that are involved with protective security policy and advice, including the Australian Security Intelligence Organization (ASIO), the Defence Signals Directorate and the Privacy Commissioner.

Protective security manual

1.19 Government policy, standards and guidelines for Commonwealth agencies are outlined in the Protective Security Manual (PSM), which was published in 1991.[1] However, except for the standards directly relating to the protection of national security information, the PSM is not binding upon agencies.

1.20 The Attorney-General's Department is currently revising the PSM. The new manual will have Cabinet endorsement and will identify security matters that are mandatory for agencies to adopt as well as those that are discretionary. The mandatory aspects will relate to the care and handling of classified information. The new manual will also include guidance on contemporary issues, including outsourcing and away-from-base work.

1.21 The Attorney-General's Department advised that an exposure draft of all eight volumes of the new manual would be issued to agencies for comment during November 1997 and that Cabinet endorsement of the manual was planned for the first half of 1998.

Policy Committee

1.22 A Protective Security Policy Committee, chaired by the Attorney-General's Department and with representatives from various agencies, was formed in 1987 to coordinate security policy in the Commonwealth. Since its inception the Committee has acted as a consultative body to consider a range

[1] Commonwealth of Australia *Protective Security Manual*, AGPS, January 1991. The manual was a replacement for earlier manuals.

of protective security policy and technical issues, eg. it approved the publication of the current PSM in 1990.

1.23 The Committee has met infrequently in recent years. It adopted a new membership and charter in June 1996, but did not meet again until September 1997 when further discussion and revision of its membership and charter occurred. The current charter is restricted to two headings, namely, 'aims' and 'objectives'. Powers and functions are covered under 'objectives', but other important aspects of a committee, including membership, method of operation and frequency of meetings are not mentioned.

1.24 The Attorney-General's Department has been reviewing the charter and is to present a revised draft more appropriately reflecting the current environment at the next meeting of the Committee in December 1997. The Department considers that it is necessary for the Committee to focus now on a range of important policy initiatives of the Government including outsourcing of information technology and the competitive tendering and contracting out of Commonwealth assets.

1.25 The ANAO considers that an effective Protective Security Policy Committee would provide an avenue for the Attorney-General's Department, as the responsible portfolio department for security policy, to establish closer links with various other Commonwealth agencies, and for other agencies to play an important consultative role in the development of new policy.

Recommendation No.1

1.26 The ANAO *recommends* that the Protective Security Policy Committee:

- decide on a charter covering the objectives of the committee, the composition and status of membership, the frequency and records of meetings, the committee's powers and functions, and accountability requirements; and
- act in accordance with the adopted charter.

Protective security within agencies

1.27 Under Commonwealth administrative arrangements, agencies are responsible for implementing their own protective security arrangements. The arrangements for each agency should be specific to its needs and will vary according to its operations, resources and functions.

1.28 The effectiveness of the protective security arrangements within each agency is highly dependant on the operation of the control framework of the

agency. As outlined in Part One, the control framework applicable to protective security arrangements covers the following elements:

- security control environment;
- security risk management;
- security control measures; and
- security monitoring and reporting processes.

The audit findings are reported under each of these headings.

Security control environment

Allocation of responsibility

1.29 Clear allocation of responsibility by chief executive officers to various levels within agencies is fundamental to effective security management.

1.30 The current PSM recommends the following minimum organisational arrangements:

- a Senior Executive Service officer be designated with responsibility for protective security matters;
- an Agency Security Adviser be allocated responsibility for the day-to-day performance of the protective security function; and
- a senior managerial level security management committee, or a similar mechanism, be established for the development, coordination and dissemination of policy, standards and procedures.

1.31 The ANAO found that security responsibilities were clearly defined in most of the agencies examined. The ANAO observed that some agencies had devolved certain security responsibilities to program and line managers. The ANAO considers that such devolution makes managers more accountable for security management and increases security awareness among staff. The revised draft PSM also recognises the importance of individual managers in achieving effective security management and accountability.

Recommendation No.2

1.32 The ANAO *recommends* that agencies review the allocation of responsibility for security with a view to devolving greater responsibility to program and line managers, whilst at the same time maintaining effective coordination through a security coordinator or similarly designated committee.

1.33 The Attorney-General's Department should also consider this recommendation in finalising the revised PSM.

Policy and staff awareness

Policy, procedures and instructions

1.34 Policy, procedures and instructions are necessary to help achieve goals and standards, and to enable agencies to respond quickly to security threats. Accordingly, they need to be clear and comprehensive and effectively communicated to, and understood by, all staff.

1.35 The ANAO found that most agencies had issued policy, procedures and instructions similar to those outlined in the PSM. However, the ANAO considered that several agencies could make improvements. Matters noted included:

- no tailoring of policy and procedures to agencies' own specific circumstances;
- procedures and instructions not issued on certain key aspects of security, such as the issue and control of identity passes; and
- a need to rationalise policy, procedures and instructions into one main security document.

Staff awareness and training

1.36 All staff have some responsibility for security. Accordingly, they should be aware of agency security policy and procedures and of their own obligations in relation to those policies and procedures. Staff awareness can be raised with education and training. The context and level of training should be tailored to match staff responsibilities.

1.37 The ANAO found that staff awareness of protective security policy and procedures, particularly in relation to information security requirements, was often lacking and needed to be raised to a higher level. In addition, the ANAO found that a large proportion of the agencies examined had not arranged adequate training for security staff, or for staff in general.

1.38 The need for improved training and awareness was highlighted by the large number of staff in some agencies who were not complying with a 'clean desk' policy, together with other weaknesses in the classification, handling and storage of information.

Recommendation No.3

1.39 The ANAO *recommends* that agencies:

- customise policy, procedures and guidelines to deal with the assessed risks applicable to their operations; and consolidate the relevant information into a readily accessible form;
- establish security competencies for staff and assess the degree of effectiveness of security training and awareness programs in operation, and;
- arrange regular formal training in protective security, including induction training for new staff, and specialised training, where appropriate; and promote and communicate security awareness through the use of demonstrations and videos, and publications and electronic means.

1.40 The ANAO considers that agency security training and awareness programs should give high priority to the requirements concerning the protection of information. The Attorney-General's Department offers a range of security training courses and workshops.

Security risk management

1.41 Determining the degree of security protection an agency may require should be a process of each agency's risk management strategy. Risk management is a process to protect against loss; it involves the identification, analysis, assessment, prioritisation, treatment and monitoring of risks.

1.42 Managing security risk involves developing a 'security plan' - a plan of action by which the agency intends to address the potential security risks. The plan should be based on the context in which the agency operates and a thorough security risk review. The ASIO and the PSCC conduct risk reviews on behalf of agencies on a cost recovery basis.

1.43 Risk reviews need to be updated and reviewed as the security environment changes. Examples of changes in the security environment include the occupation of new buildings, a policy enabling home based work, and technological developments.

1.44 The ANAO found that all agencies had undertaken some form of risk review. Some of the reviews, however, were not comprehensive, in that they did not cover all resources, or link security risks with other operational risks faced by the agency; furthermore, some reviews needed updating for changes in the security environment. The ANAO also found that some agencies had no formal planning to address the identified risks.

Recommendation No.4

1.45 The ANAO *recommends* that agencies without comprehensive and up-to-date security risk assessments and planning:

- undertake security risk reviews and assessments as part of their risk management process, seeking expert assistance as required;
- develop security plans outlining the activities and resources (costs) necessary to address the identified risks; and
- review and update the security risk assessments and plans at set intervals, eg. three yearly, annually, or when circumstances require it, ie. changes in the security environment.

1.46 The revised draft PSM includes a volume titled 'Managing Security Risk'. This volume should enable agencies to conduct comprehensive risk assessments.

Security control measures

1.47 Security control measures comprise information security, personnel security, physical security, and computer and communications security (not covered by this audit).

Information security

1.48 Information security arrangements refer to the identification, marking, handling, storage and disposal of classified material. Classified material is official information, intellectual property or assets requiring protection under either 'national security' or 'sensitive' classifications[2].

1.49 The ANAO found inconsistencies in the identification and marking of classified information at several agencies, including incorrect classification and no review of documents to see if the classifications remained appropriate. The ANAO also found weaknesses in the handling and storage of classified information at a number of the agencies, including:

- no controls over the copying of documents;
- lack of appropriate storage facilities and locking devices; and
- combination locks not changed at the required frequency.

Instances were also noted where information was stored in facilities which were more secure than required.

[2] The classification system used by the Commonwealth is briefly described in Appendix 1.

Personnel and physical security

1.50 Personnel security is concerned with the suitability of people requiring access to classified information, valuable assets (in terms of both cost and qualitative factors, such as importance to operations) and secure areas. Physical security comprises the physical measures taken to prevent unauthorised disclosure or loss of material, and tampering with or damage of assets, and the protection of staff from violence and abuse.

1.51 The ANAO found that personnel and physical security were well controlled at most agencies. However, there was a need for some agencies to improve physical security controls relating to visitor records, identification passes and after hours access.

Security monitoring and reporting processes

1.52 As part of good governance, executive management should establish a control and monitoring framework to ensure that the security policies, instructions and procedures of the agency are implemented and operating as intended. This would normally involve a program to identify breakdowns in policies and procedures, reporting of performance to appropriate levels of management, and implementation of corrective action, as necessary. Such a framework would also need to be closely linked with the risk reviews discussed earlier.

1.53 The ANAO found that security incidents were often recorded and filed without management review. There were also instances where records of security inspections were not maintained and where automated records, eg. after hours entry to buildings, were not reviewed. As a result of these breakdowns, investigations of actual and potential security incidents, and analysis of the number, nature and distribution of such incidents, were not always performed, or reported to executive management. In addition, program managers generally had no responsibility to report on security management.

Recommendation No.5

1.54 The ANAO *recommends* that agencies:

- maintain systems to record key data on all security incidents and promote the use of the systems to staff;
- investigate security incidents as they arise and monitor the causes and consequences of incidents on an ongoing basis; and
- provide reports on the performance of security operations to executive management at set intervals, eg quarterly, monthly.

Canberra ACT
4 December 1997

P. J. Barrett
Auditor-General

Part Three

Appendices

Appendix 1

Background and contextual information

What is protective security?

Protective security is the protection of information, assets and people from potential threats and dangers. It involves the identification, assessment and review of risks, and the implementation and maintenance of security measures; and covers physical security (eg building access control), personnel security (eg police record checks on new staff), information security (eg classification and storage of documents), computer and communications security (eg password protection and encrypted messages) and personal safety (eg protection against bomb threats).

The term 'protective security' does not generally cover protection against fire, natural disasters, and work accidents. These areas, although closely aligned with protective security are dealt with separately within the Commonwealth. In addition, fraud control, although encompassed within protective security, is administered separately. Table 1 shows the relevant areas of Commonwealth policy responsibilities.

Table 1
Protective security and related threats - Commonwealth policy responsibilities

Threats	Responsible Agency (Portfolio)
Protective security	Attorney-General's Department
Fraud control	Commonwealth Law Enforcement Board (Attorney-General's Portfolio)
Fire safety	Commonwealth Fire Board (Finance and Administration Portfolio)
Natural disasters	Emergency Management Australia (Defence Portfolio)
Work safety	Safety, Rehabilitation and Compensation Commission (Workplace Relations and Small Business Portfolio)

Protective security in the Commonwealth

Commonwealth agencies maintain significant quantities of assets and information on behalf of the Government and collectively have large numbers of clients and staff. These agencies are entrusted with protecting information, assets and people from various threats and dangers. For example, national security or trade information may be of interest to foreign governments; commercial or personal information may be of interest to business entities or individuals; physical assets may be subject to theft or

sabotage; and counter staff may be subject to abuse or physical attack. Protection of information,

assets and people must be balanced, however, with each agency's responsibilities for accessibility, openness and accountability.

Information is generally seen as the key item requiring protection because of its importance to Government decision making, and as its protection is required under various pieces of legislation, eg the *Crimes Act 1914*, the *Public Service Act 1922*, and the *Privacy Act 1988*. However, in particular circumstances, the protection of assets and people are just as important. The level of risk varies from agency to agency, and consequently, each agency is responsible for establishing protective security arrangements commensurate with its operational responsibilities and environment.

Central agency arrangements

The Government, through the Attorney-General's Department, has developed policies, standards and guidelines for sound protective security management within Commonwealth agencies. These are outlined in a protective security manual. The Attorney-General's Department is also responsible for privacy policy and provides security advice, training and vetting services.

The Government also has a number of specialist agencies concerned with protective security; these agencies and their responsibilities relating to protective security are listed in Table 2.

Table 2:

Other Commonwealth agencies with protective security responsibilities

Agency	Responsibilities
Australian Security Intelligence Organization	Intelligence activities relating to national security; testing and endorsement of security equipment and products; providing national security advice to agencies; and promoting general awareness of security issues.
The Defence Signals Directorate	Provision of advice on computer and communications security.
The Privacy Commissioner	Operation of the Privacy Act; this includes the provision of policy and guidance to agencies and the handling of complaints relating to privacy.
Australian Archives	Preservation of Commonwealth records of administrative, community, legal and research value.
Australian Protective Service	Provision of security and custodial services to Government agencies (on a fee for service basis).

Other central documentation

The Attorney-General's Department also issues protective security bulletins. In addition, other relevant documentation includes the Privacy Commissioner's guidelines for the protection of personal information and ASIO's security equipment catalogue (last edition in 1997).

Classification system

Official information and assets requiring protection need to be classified according to a classification system. The classification system used in the Commonwealth comprises TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED for national security material and HIGHLY PROTECTED, PROTECTED and -IN-CONFIDENCE for sensitive material. The national security classifications are long standing and are used by other countries. The first two mentioned sensitive classifications were introduced in 1990. Agencies are to classify relevant material into these categories.

Changing environment and recent initiatives

The security environment has not remained static. Changes in the security environment over recent years have included:

- a moderation in the threat of political espionage since the ending of the *cold war*;
- an increase in *industrial* espionage;
- increased emphasis on *privacy* since the establishment of the Privacy Act (1988);
- *technological* advances in information storage, administrative arrangements and security equipment;
- *outsourcing* of government services; and
- *workplace changes*, eg home based work, portable computers.

Current and recent Commonwealth initiatives on protective security include:

- a revision of the protective security manual with a new manual planned for issue in 1998; and
- the establishment of the Australian Security Vetting Service within the Attorney-General's Portfolio during 1996 to conduct personnel security clearances on behalf of other agencies on a user pay basis.

Previous public reviews

Protective security in the Commonwealth was subject to a major public review in the 1979 Enquiry into Protective Security undertaken by Mr Justice Hope. This enquiry resulted from the bombing of the Sydney Hilton Hotel during a regional meeting of Commonwealth Heads of Government in February 1978.

Following on from the Hope Enquiry, the ANAO commenced a program of protective security audits from the early 1980's. The most recent ANAO reports on protective security issues were in 1993-94 and 1994-95.[3]

In March 1994 the Parliamentary Joint Committee on the Australian Security Intelligence Organization issued a report titled *A review of security assessment procedures*. The Committee recommended a number of changes to the procedures, including some with application to agencies. The Government's response to the report accepted most of the recommendations.

In June 1995 the House of Representatives Standing Committee on Legal and Constitutional Affairs issued a report entitled *In Confidence: A report of the inquiry into the protection of confidential personal and commercial information held by the Commonwealth*. The report concluded that the protection given to such information was neither comprehensive nor reliable.

An official response to the 'In Confidence' inquiry had not been presented at the time of preparation of this report.

The Privacy Commissioner conducts audits of Commonwealth agencies to determine the extent of compliance with the Privacy Act; summaries of the results of the audits are published in the annual reports of the Commissioner. The Privacy Commissioner also undertook a survey on computer security during 1994.[4]

---

[3] The reports included Audit Report No.1, 1993-94 *Report on Ministerial Portfolios Budget Sittings 1993*, Volume 2 Cross-portfolio Audits, Audit Report No.23, 1993-94 - Efficiency Audit Department of Social Security - *Protection of Confidential Client Information from Unauthorised Disclosure,* as well as reports on computer security. The first mentioned report examined protective security across a number of agencies.

[4] Refer Annual Report on the Operation of the Privacy Act 1994-95 p. 85-89.

Appendix 2

Audit objectives, criteria, scope and approach

Audit background

The Hope Enquiry's May 1979 report recommended a role for the ANAO in evaluating protective security in government agencies. In May 1980 the Government accepted the recommendation of the Enquiry and the Auditor-General subsequently agreed that the ANAO would undertake audits of protective security.

In the 1980's and early 1990's, the ANAO conducted protective security audits in many agencies. These audits were conducted in accord with audit guidelines, which were developed by the ANAO in liaison with the Australian Security Intelligence Organization. The audits were usually conducted on an individual agency basis and were reported independently from each other; in 1993, the results of reviews across a selection of agencies were reported together.

In addition, during the 1990's, the ANAO commenced undertaking audits of computer security at selected agencies with extensive information technology operations.[5]

Audit objectives

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

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

The audit did not include computer security and communications security, as they are considered specialised subjects worthy of separate independent audit coverage. In this regard the ANAO has recently reported an audit on Internet security across a number of agencies (Audit Report No.15 1997-98 refers).

The audit covered security management and administration at thirteen individual agencies and the central agency role of the Attorney-General's Department relating to protective security. The audit did not extend to the roles of the ASIO and the Privacy Commissioner.

[5] ANAO reports on computer security include Audit Report No.2, 1993-94 Australian Bureau of Statistics, Audit Report No.31, 1994-95 CSIRO and Audit Report No.6, 1994-95 Australian Taxation Office.

Audit criteria

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

- *security control environment* - agencies would be expected to have allocated responsibility for protective security to appropriate personnel, developed and implemented a broad agency policy document and operational procedures and instructions to enable the implementation of policy, appointed a trained security adviser, and implemented and maintained staff training and awareness programs;
- *security risk management* - agencies would be expected to have a security plan based on a properly conducted and up-to-date threat assessment and subjected to periodic review;
- *security control measures* ie. systems in operation for maintaining physical security, personnel security, and information security - agencies would be expected to have operational programs and systems for maintaining the various forms of security; and
- *security monitoring and reporting processes* - agencies would be expected to have monitoring and reporting processes to ensure policies are adhered to, procedures are properly applied and that risks are managed.

Audit approach

The audit was conducted in accordance with ANAO Auditing Standards and was undertaken during the early part of 1997. The main elements of the audit approach were:

- revision and updating of the protective security audit guidelines to reflect current circumstances;
- completion of field work in accord with the revised audit guidelines at thirteen agencies including some regional operations;
- analysis of agency information with a view to reporting best practice;
- liaison with the Attorney-General's Department and review of security policy and training;
- the issue of a report to all agencies highlighting the better practices observed and proposing recommendations for improvement; and
- the issuing of reports to the relevant Ministers.

The cost of the audit was $416 500. The average cost of the field work undertaken at each of the 16 agency locations was $19 000.

Appendix 3

Security management in Commonwealth agencies - better practice principles

Introduction

Security management covers the policies, practices and processes of an organisation to protect its functions and resources (ie. information, assets and people) from the threats and dangers of espionage, theft, sabotage, vandalism and other criminal activity.

Commonwealth agencies perform functions and maintain resources on behalf of the Government and the Australian community. In doing so, they are, among other things, accountable for their performance in security management, and must therefore implement and maintain a protective security program specific to their needs.

This appendix has been prepared to assist public sector managers achieve an effective security management program. It outlines the better practice principles and success factors considered desirable for effective security management.

In developing these better practice principles and success factors, the ANAO has taken into account the guidance provided by the current drafts of the proposed new issue of the Commonwealth Protective Security Manual, as well as other existing guidance. However, the ANAO guide is only a brief synopsis of better practice principles and success factors for security management, and needs to be used in conjunction with the new manual when it comes into production, and with other current central agency guidance.

Security management principles

The security management principles developed by the ANAO are as follows:

- Security is integrated with strategic planning and organisational arrangements.
- Security planning focuses on real and significant risks.
- Resources are protected in line with their value and vulnerability.
- Staff are aware of agency expectations and their own responsibilities.
- Security arrangements are assessed on an ongoing basis.

The *Success factors* and *Outcome* relating to each of these principles are outlined on the following pages.

Strategic Planning and Organisation

Principle

Security is integrated with strategic planning and organisational arrangements.

Success factors

- Corporate plan promotes the protection of agency resources and functions.
- Risk management plan integrates security with other operational risks.
- Business and operational plans recognise security management and accountability requirements at the program level.
- Disaster recovery plans enable continuity of operations.
- Contractual arrangements reflect the agency's security requirements.
- Overall responsibility for security is coordinated by executive management.

Outcome

Security management will be consistent with the agency's goals and objectives.

Risk Management

Principle

Security planning focuses on real and significant risks.

Success factors

- All resources/functions requiring protection and the risks to those resources are identified.
- Risks are analysed to establish the consequences and the likelihood of their realisation.
- Risks are allocated priorities for treatment according to established risk criteria.
- Existing and alternate security control measures are assessed on performance and cost.
- Security plans are interlinked with fraud, emergency and safety plans.
- Security risk assessments and plans are updated periodically or as circumstances change.

Outcome

Security measures will address the level of risk in a cost efficient and effective manner.

Control Measures

Principle

Resources are protected in line with their value and vulnerability.

Success factors

- Resources are made available on a ‘need-to-know’ basis.
- Resources are classified in accord with an established classification system and for a limited time.
- Standards are established for the use, storage, back up, transmission and disposal of classified resources.
- Personnel requiring access to classified resources are vetted by qualified officers.
- Access to facilities, including information technology and communications systems, is restricted to authorised personnel.
- Personal security is provided where staff are at risk.
- Suitable storage and transmission facilities are installed to meet the established standards for protecting classified resources.

Outcome

Security measures will facilitate and enhance the performance of agency functions and services, and ensure the integrity and continuity of the agency’s operations.

Staff Awareness and Responsibility

Principle

Staff are aware of agency expectations and their own responsibilities.

Success factors

- Security policy and standards are promulgated by executive management.
- Program and line managers are responsible for managing the protection of resources under their control.
- Security procedures and instructions are comprehensive, up-to-date, readily accessible and easy to understand.
- New staff are educated in security policy and procedures either at induction courses or through the provision of security awareness kits.
- Security awareness is promoted among staff through the regular conduct of security training and other promotional activities.

Outcome

Policy and procedures will be understood and practised by staff.

Monitoring and Reporting

Principle

Security arrangements are assessed on an ongoing basis.

Success factors

- Audit trails are used where practicable.
- Security incidents are promptly identified, reported, investigated and acted upon.
- Statistical analysis and evaluation of incidents is undertaken on a regular basis.
- Reports on security operations are provided to executive management periodically.
- Internal audit undertakes reviews of security operations.
- Organisational arrangements, risk management and security measures are revised as necessary.

Outcome

Management will be responsive to breakdowns in security policy and procedures, and changes in the security environment.