The Auditor-General

Audit Report No.7 1999–2000
Protective Security Audit

Operation of the Classification System for Protecting Sensitive Information

Australian National Audit Office

ISSN 1036-7632

ISBN 0 644 39106 5

Australian National
Audit Office

Canberra ACT
11 August 1999

Dear Madam President
Dear Mr Speaker

The Australian National Audit Office has undertaken a protective security audit in accordance with the authority contained in the *Auditor-General Act 1997.* I present this report of this audit, and the accompanying brochure, to the Parliament. The report is titled *Operation of the Classification System for Protecting Sensitive Information.*

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

Yours sincerely

P. J. Barrett
Auditor-General

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

AUDITING FOR AUSTRALIA

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

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

The Publications Manager
Australian National Audit Office
GPO Box 707 Canberra ACT 2601

Telephone (02) 6203 7505
Fax (02) 6203 7798
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

Peter Green
Grace Guilfoyle
Andrew Greaves

Contents

Introduction and Summary

1. Introduction and summary

Audit context

1.1 Information is a major resource of most Commonwealth organisations, mainly because of its importance to Government decision making and program management. Accordingly, its protection is of paramount importance. Its protection is covered by various legislative requirements including the *Crimes Act 1914*, the *Public Service Act 1922* and the *Privacy Act 1988*, as well as about 150 other Acts relating to specific types of information.

Commonwealth policy

1.2 Commonwealth policy in relation to protective security of information is contained in the Protective Security Manual (PSM)[1]. The PSM is supplemented in relation to Information Technology and Telecommunications (IT&T) security by Defence Signals Directorate (DSD) publications, in particular, Australian Communications-Electronics Security Instructions (ACSI) 33 and 37[2].

Classification system

1.3 The Commonwealth operates on the basis that *sensitive information*, that is, information, which, if compromised, *could cause harm* to the nation, the public interest, the government or other entities or individuals, should be *classified* according to a *classification system*.

1.4 The classification system for sensitive information in the Commonwealth has two categories, namely, *national security* (eg. defence and international relations) and *non-national security* (eg. commercial and personal).

1.5 There are seven classification levels within these categories, as shown in Table 1. Each level signifies the respective value of the information (ie. the degree of harm that could result from its compromise) and the relevant security measures required to protect the information.

---

[1] The current manual was first published in January 1991; a revised manual is expected to be published in 1999. It comprises eight volumes including one titled *Information Security*. A listing of the eight volumes is provided at Appendix 5.

[2] ACSI 33 is titled *Security Guidelines for Australian Government IT Systems*; the current edition was issued in April 1998. ACSI 37 is titled *Australian Government Standards for the Protection of Information Technology Systems Processing Non-National Security Information at the Highly Protected Classification*; it was first issued in June 1998.

Table 1

Classification system—levels of classification[3]

Level of security	*National security information*	*Non-national security information*
Low	Restricted	'X'-in-Confidence
Medium	Confidential	Protected
High	Secret	Highly Protected
Very High	Top Secret	—

Notes:

(1) The PSM uses the term 'X-in-Confidence' where 'X' represents the context of the information, eg. Staff-in-Confidence, Commercial-in-Confidence and Security-in-Confidence.

(2) The level of protection required by the PSM is approximately equal for the classifications shown in each row eg. Confidential is approximately equal to Protected.

Unauthorised use of Commonwealth information

1.6 Sensitive information must be protected from unauthorised use and/or disclosure. The extent of unauthorised use of Commonwealth information is unknown, other than for unauthorised disclosures reported by the media. At least 56 cases of unauthorised disclosure have been recorded in recent years (see Appendix 2). It is also likely that many more incidents than those recorded are actually occurring.[4]

Previous audit coverage

1.7 The audit was a follow-on to *Audit Report No. 21, 1997–98, Protective Security* which reviewed, among other things, information security other than computer and communications security, against the policy and procedures outlined in the 1991 PSM. That audit found inconsistencies in the identification and marking of classified information and weaknesses in the handling and storage of classified information as well as other breakdowns impacting on information security. A summary of the audit is provided at Appendix 3. A further audit report, *Audit Report No. 15, 1997–98, Internet Security Management* also served as a forerunner to the current audit.[5]

---

[3] Note: a description of the Commonwealth's classification system is provided at Appendix 1—'Classification System—How to classify information'.

[4] This assessment is supported by the findings of the British Government's 1996-97 annual report on the *Unified Incident Reporting & Alert Scheme, IT Security in Government.*

[5] A brief description of *Audit Report No. 15, 1997-98, Internet Security Management* is provided in Appendix 4.

Audit objectives, scope and criteria

Audit objectives

1.8 The main objectives of the audit were:

- to determine whether organisations are *protecting the confidentiality of sensitive information* in accordance with the Commonwealth's security classification system, related Government policy and standards, and recognised best practice; and
- to recommend improvements as necessary, including those that could be applicable to all organisations.

Audit scope

1.9 The audit covered both paper-based and computer-based information and involved aspects of physical and personnel security, in addition to information security. However, it did not attempt to provide an opinion on all aspects of security in the organisations examined.

1.10 The audit was undertaken at six organisations which operate under either the *Financial Management and Accountability Act 1997* or the *Commonwealth Authorities and Companies Act 1997*.

1.11 In terms of information resources, the organisations fitted into two different categories, with three organisations in each category. The categories were:

- those with a range of national security and non-national security information at all classification levels (hereafter referred to as Category A organisations); and
- those with a significant proportion of low level non-national security information (ie. 'X-in-Confidence' information) and small amounts of sensitive information at higher classified levels (hereafter referred to as Category B organisations).

1.12 None of the organisations covered was included in the previous audits. For security reasons, the organisations are not named in this report.

1.13 Several of the organisations had a significant amount of sensitive information resources. This assessment was based on the number of classified paper files maintained. Classified files at each organisation commonly represented more than 40 per cent of total files. All of the organisations also held sensitive information electronically with two organisations operating secure networks and two others operating mainframe environments with large data bases.

1.14 The main focus of the audit was on the identification of material requiring protection and on the administrative security arrangements and controls for protecting classified paper-based and computer-based information.

Evaluation criteria

1.15 The 1991 PSM was still in force at the date of preparation of this report. However, a revised PSM, which was first issued as an exposure draft in December 1997 and is still in draft form, was used as a guide in assessing the performance of each organisation, given its currency. Accordingly, unless otherwise indicated, all references to the PSM in this report are to the August 1998 draft of the revised PSM, that is, the version available at the time of commencement of the audit, in October 1998. Due to its continuing draft status, the revised PSM has been subjected to minor revision since the commencement of the audit, and may be further revised prior to finalisation. ACSI 33 was the main supplementary guide used in relation to IT&T security.

1.16 The information security processes and practices in place in the organisations reviewed were assessed against a model of effective internal control adapted from the framework developed by the Committee of Sponsoring Organisations of the Treadway Commission[6].

1.17 An effective *information security control structure* was defined in terms of the following inter-related elements:

- risk management;
- control environment;
- control measures; and
- monitoring and review processes.

Audit evaluation criteria were established under each element as indicators of the type and nature of information security controls expected to be in place.

1.18 Further information relating to the audit background, objectives, criteria and approach is provided at Appendix 4.

---

[6] *Internal Control – Integrated Framework*, American Institute of Certified Public Accountants, 1992.

Audit opinion

1.19 In the opinion of the ANAO, all organisations covered by the audit were not adequately *protecting the confidentiality of sensitive information* in accordance with the Commonwealth's security classification system, related Government policy and standards, and recognised best practice. While the extent of the breakdowns in information security varied among the organisations, the more common and serious breakdowns related to risk assessments and planning, allocation of responsibility, IT&T networks, security clearances, staff training and awareness, and monitoring and review activities. As a result, there was a high risk of unauthorised access to sensitive information within most of the organisations examined. This was particularly so in relation to staff and other people dealing with the organisations, such as contractors and clients. This level of risk is considered significant given the nature of the information and the likely consequences, if it were misused.

1.20 The ANAO considers that all of the organisations examined need to improve their information security arrangements in order to protect sensitive information in accordance with the requirements of the PSM. On this basis, the ANAO has made a number of recommendations to assist all Commonwealth organisations achieve better performance in information security management.

Audit findings

1.21 The significant issues arising from the audit are summarised below. Chapter 2 of this Report discusses each of these issues in detail within the context of each element of the information security control structure defined above. Failure to address these matters increases the likelihood that sensitive information will be improperly accessed and/or disclosed.

Risk management

1.22 The audit found that, while risk assessments had been performed, they did not address in sufficient depth the issues relating to information security. Consequently, most of the organisations examined had not clearly identified the nature, extent and value of the sensitive information resources that they held, or all the risks associated with those resources. Furthermore, risk assessments were either out of date (eg. organisational circumstances had changed), or they were incomplete (eg. they did not include all locations or excluded IT&T). As well, the organisations did not generally have an overall security plan to address information security risks.

Control environment

1.23 The findings related to four main issues, namely governance arrangements, security clearances, the IT&T environment, and staff awareness and training.

Governance arrangements

1.24 Improved information security requires a higher level of interest and attention from senior management of Commonwealth organisations. In particular, the audit found there was a need for higher level direction and review of security matters, preferably, where practicable, through an executive management committee.

1.25 A key aspect of this oversight role is to achieve more effective integration of IT&T security with other security activities to enable a comprehensive and consistent approach to the protection of sensitive information resources.

Security clearances

1.26 A high proportion of staff had security clearances above the level that their work commitments would require. While these arrangements are likely to have a positive effect on the overall level of personnel security, they come at a cost, with a consequent impact on efficient resource use.

1.27 However, of greater concern from a security effectiveness perspective, was that a number of staff had access to information for which they were not appropriately cleared.

1.28 As a consequence of the long lead times to obtain clearances, commonly up to three months, the ANAO found that officers obtained access to information before they were cleared, or without a clearance being initiated. The latter applied particularly in the case of temporary staff and contractors.

1.29 The ANAO also found that most organisations did not maintain the currency of their security clearances, compounding the above situation. A key underlying reason for this was the lack of consolidated management information on security-cleared positions, the occupants of those positions, or the level and currency of their clearances.

IT&T environment

1.30 The access management controls on Local Area Networks (LAN) were often not configured or implemented in accordance with the requirements of ACSI 33. Areas requiring attention included passwords, the number of log-on attempts, and inactive user accounts. These weaknesses are of concern as all the networks carried sensitive information.

Staff awareness and training

1.31 Organisations did not have a clear strategy to address staff training and awareness issues relating to information security. In addition, in most organisations there was insufficient training provided to staff responsible for creating and handling sensitive information.

Control measures

1.32 The adequacy of the control environment has a direct influence on the operation of security control measures established by management. Where the environment is not effective, there is a consequent higher risk that the controls established by management will not operate as intended. This was found to be the case in this audit.

1.33 In many instances, the control measures were not well applied or were not as effective as management expected. Many staff did not have a detailed understanding of the classification system which resulted in sensitive information being incorrectly classified or not classified at all. All organisations incorrectly classified files with over-classification being the most common occurrence. Over-classification has the effect of increasing the costs of protection and restricting the flow of information within the organisation.

1.34 Documents were often not provided with protective markings to indicate the level of protection required. There was a need for each organisation to consider the marking of documents in conjunction with the assessed risks and other protective controls in place. In addition, there were breakdowns in relation to the storage and transmission of sensitive information which increased the risk of unauthorised access and/or disclosure of the information.

Monitoring and review processes

1.35 The audit found that more attention needs to be given to establishing effective monitoring and review processes, particularly in relation to IT&T audit trails, to ensure security policies and procedures are operating as management intended. Some organisations did not have a monitoring and review framework, and, accordingly, senior management was unaware of the level of security compliance/awareness that existed.

Better practice

1.36 The ANAO considers that the PSM and related publications provide a better practice framework for protective security within the Commonwealth. In addition, Appendix 3 of *Audit Report No.21, 1997–98* outlined better practice principles for security management.

1.37 The expected release of the revised PSM should create an ideal opportunity for raising the awareness of all aspects of protective security and encouraging improvements in security management within Commonwealth organisations.

1.38 In relation to information security, implementation of the recommendations of the current audit and the three reviews referred to below, should lead to improved performance across Commonwealth organisations.

Concurrent reviews

Office for Government Online (OGO)

1.39 The Office for Government Online (OGO) was recently tasked to undertake a review of security surrounding the storage of electronic documents within Commonwealth organisations and the transmission of such documents between organisations. The review was conducted by a working party with representatives from a number of departments and a draft report was provided to the Secretaries of the Departments in late June 1999. The outcome of this review should provide further recommendations, including technical solutions, for improving the security of Commonwealth information.

Protective Security Coordination Centre (PSCC)

1.40 A comprehensive review of personnel security within the Commonwealth, including review of security clearance procedures, is currently being conducted by the Protective Security Coordination Centre (PSCC) of the Attorney-General's Department and other member organisations of the Protective Security Policy Committee (PSPC).[7] The review is expected to be completed by the end of 1999.

Inspector-General of Intelligence and Security

1.41 The Inspector-General of Intelligence and Security is currently conducting a review relating to unauthorised disclosures of sensitive information.

Reports to organisations

1.42 Each of the audited organisations was issued with a comprehensive report comprising an executive summary and detailed report outlining the audit conclusions, findings and recommendations applicable to each organisation. The organisations received the audit reports in a cooperative manner and provided positive responses to the individual findings and recommendations. In addition, each of the organisations advised of proposed remedial action.

---

[7] The PSPC is an inter-departmental committee chaired by the PSCC to coordinate security policy in the Commonwealth.

1.43 The ANAO sought comment from the audited organisations and organisations with security policy and coordination responsibilities on the generic findings and recommendations outlined in this report. The ANAO considered the responses of the various organisations in developing the final report. The organisations accepted the overall content and recommendations of the report.

Recommendations

1.44 The above issues echo the broad findings arising from *Audit Report No. 21, 1997–98, Protective Security*. The continuing breakdowns in performance demonstrate the need for organisations to devote more attention to protective security arrangements, and, in this instance, to information security in particular. To make a difference, senior management support for improved protective security arrangements will be required.

1.45 The nature of the issues raised indicates that they would have wider coverage across the Commonwealth. Accordingly, the following audit recommendations are directed to all Commonwealth organisations that hold sensitive information. All such organisations should consider the recommendations in the context of the revised PSM and the risks involved.

Risk management

Recommendation 1

1.46 The ANAO *recommends* that organisations develop a security risk assessment policy and framework for the whole of their organisation and undertake a security risk assessment in relation to information security (including IT&T). The policy and framework should, among other things, establish the degree of risk that the organisation is prepared to accept and the likely frequency of review and methodology to be used for each assessment. The risk assessment should, among other things:

- identify all information resources;
- identify all the risks to information resources, ie. leaks, theft, sabotage, fraud, as well as the likely perpetrators;
- assess the consequences and likelihood of the risks occurring;
- determine the level of protection that is required for sensitive information; and
- allocate priority for the treatment of the identified risks.

(paras 2.9 to 2.15 and 2.22 refer)

Recommendation 2

1.47 The ANAO *recommends* that, following completion of the risk assessment, organisations develop and implement an integrated security plan to ensure sensitive information is classified and protected on an ongoing basis in accordance with Government requirements and policies specific to the organisation. Such a plan should cover the allocation of responsibility and staff resourcing requirements; the review and maintenance of staff security clearance requirements; the conduct of staff awareness programs; the acquisition of security equipment; an analysis of security controls relating to each of the IT&T systems; and the development, operation and maintenance of monitoring activities (for both paper-based and computer-based information).

(paras 2.16 to 2.22 refer)

Control environment

Recommendation 3

1.48 The ANAO *recommends* that organisations:

- integrate the physical and IT&T security functions and responsibilities by, for example, placing the ASA and the ITSA together under one management (and as far as practicable, the ITSA outside of the IT operations branch / section); and
- coordinate the management of all security activities through an appropriate executive responsibility, that is, either enabling an existing management committee or establishing a security committee (or similarly designated committee which may include associated activities eg. privacy), to take responsibility for providing direction and review of security matters (risk assessment, policy, network protection, security cleared positions, integration of security functions, staff awareness program, performance measurement, etc).

(paras 2.30 to 2.42 refer)

Recommendation 4

1.49 The ANAO *recommends* that organisations:

- as part of the security risk assessment, determine which positions require security clearances and ensure staff occupying those positions have the required level of clearance. This also applies to other personnel who have access to sensitive information or the premises on a regular and an unescorted basis, (eg. contractors, cleaners and maintenance workers); and
- monitor clearance levels at least annually and ensure supervisors are aware of each staff member's clearance level; and provide regular

reports on the status of security clearances to the executive (ie. management committee responsible for security, or other similar arrangement).

(paras 2.44 to 2.61 refer)

Recommendation 5

1.50 The ANAO *recommends* that organisations:

- review current IT&T networks and applications that process sensitive information, and implement any changes necessary to meet the recommendations outlined in ACSI 33; and
- obtain executive approval for the processing of sensitive information on an IT&T system based on the certification of the system for such purposes by a suitably qualified certification authority.

The development of new networks and applications should also ensure proper security in accordance with ACSI 33. Where the organisations currently process or plan to process sensitive information on electronic systems at the 'Highly Protected' classification level or higher, the organisations should consult ACSI 37 and / or the Defence Signals Directorate.

(paras 2.63 to 2.71 refer)

Recommendation 6

1.51 The ANAO *recommends* that organisations:

- implement a formal staff training and awareness program, which includes, among other things, on-the-job training in the use of the classification system and structured training in IT&T information security; and
- establish a means of assessing the effectiveness of the training and awareness program.

(paras 2.73 to 2.76 refer)

Control measures

Recommendation 7

1.52 The ANAO *recommends* that organisations:

- evaluate which documents, forms and data require classification under the requirements of the PSM, and implement procedures to assist in ensuring proper application of the classification system; and
- identify specific examples of classified material in the context of their operations and conduct relevant training in the application of the classification system.

(paras 2.83 to 2.87 refer)

Recommendation 8

1.53 The ANAO *recommends* that organisations:

- develop electronic document templates which include the protective markings as headers and footers;
- encourage the use of time-limited classifications; and
- ensure that sensitive documents received from other organisations or individuals are marked with the relevant Commonwealth classification on all pages.

(paras 2.89 to 2.93 refer)

Recommendation 9

1.54 The ANAO *recommends* that organisations:

- reassess the adequacy of storage requirements and facilities for sensitive information in terms of the PSM;
- implement a clear desk policy to encourage the protection of sensitive information;
- ensure staff have access to appropriate physical and electronic facilities for storing and transmitting sensitive information; and
- require screen saver passwords to be used on all computer workstations.

(paras 2.95 to 2.99 refer)

Monitoring and review processes

Recommendation 10

1.55 The ANAO *recommends* that organisations develop a formal security monitoring and review program, incorporating both physical and IT&T security aspects. The program should be utilised to analyse areas of security weaknesses, highlight procedural deficiencies and/or identify where the policies and practices require revision. Such a program could include periodic after-hours inspections, regular reviews of all IT&T system audit trails, periodic electronic searches of departmental LANs and personal computer hard drives, and periodic examination of file classifications. Organisations should also develop clear procedures for dealing with offenders. This could involve various internal disciplinary measures and the incorporation of breach incidents as a performance measure in performance agreements.

(paras 2.104 to 2.114 refer)

Detailed Audit Conclusions, Findings and Recommendations

2. Detailed audit conclusions, findings and recommendations

Introduction

2.1 This chapter of the report discusses the audit findings in the context of each element of the protective security *control structure*. It provides a separate conclusion on the effectiveness of each component of the control structure assessed against the evaluation criteria for that component. It then outlines the detailed audit findings requiring management action and recommendations for all organisations to consider.

Control structure

2.2 The control structure in an organisation provides an important linkage between strategic objectives and the functions and tasks undertaken to achieve those objectives. It is fundamental to good corporate governance that the control structure is well designed, implemented and monitored to ensure it operates as management intended.

2.3 The control structure is made up of the following interrelated components:

- risk management;
- control environment;
- control measures; and
- monitoring and review processes.

Management information systems and communication processes overlay these elements. The interaction between these components is critical to the effectiveness of the control structure.

2.4 The control structure model can be applied to most administrative arrangements including information security.

Risk management

2.5 All organisations, regardless of size or nature, encounter some form of risk that can adversely impact on the achievement of its objectives. Assessing risk is a major component of an effective control structure. It involves the identification, analysis, assessment and prioritisation of risks that need to be treated by control activities.

Evaluation criteria

2.6 In relation to effective risk management of information security it is expected that each organisation would have:

- assessed the value of all information resources and the likely risks to those resources;
- determined which information resources require protection under the Commonwealth's classification system; and
- developed an information security plan to protect its sensitive information resources.

These processes would normally be based on the conduct of periodic risk assessments.

Overall audit conclusion and main findings

2.7 Most of the organisations reviewed had not clearly established which information resources required protection under the Commonwealth's classification system or the levels of protection that would be appropriate. The identification and protection of sensitive information was therefore often reliant on the individual staff dealing with the information, which sometimes resulted in inconsistencies in the application of the classification system.

2.8 The main findings requiring management action were:

- incomplete and out-of-date risk assessments;
- no formal identification of the nature, extent and intrinsic value of information resources, or the risks associated with those resources; and
- a lack of security planning.

Detailed audit findings and recommendations

Risk assessments

2.9 A properly conducted and up-to-date risk assessment is fundamental to the security of an organisation. It should be used as the basis for all security management.

2.10 Volume B of the revised PSM provides a useful reference for conducting security risk assessments. Professional advice may be necessary for many, if not most, organisations.

2.11 All organisations reviewed had conducted a risk assessment, but most had not addressed information security in any depth. The risk assessments undertaken applied to the security of assets and people as well as information resources.

2.12 Several of the assessments were incomplete (eg. only covered particular geographic locations; did not include IT&T) or out of date (eg. more than five years old; significant subsequent changes to the organisation's environment). In addition, most of the organisations had not established a clear policy in relation to security risk assessments regarding such matters as coverage, methodology and frequency.

2.13 None of the organisations had identified the nature and extent of the classified information resources held and two of the organisations were unable to generate the numbers of files at the various security classification levels. None of the organisations was able to estimate the amount of classified information held electronically.

2.14 It was difficult to ascertain the level of threat faced by each organisation other than for unauthorised disclosures as published by the media. At least three of the organisations had been affected by known leaks of sensitive information.

2.15 Most organisations had given minimal attention to the identification of particular threats or the likely perpetrators of threats. Further, some of the organisations had given little consideration to additional threats arising from the development and expansion of their IT&T operations. However, all the organisations recognised the need for strong perimeter security, while others also focused on high levels of personnel security. In these circumstances, the ANAO considered that the threats for most organisations were likely to come directly from staff or through contact with staff.

Information security planning

2.16 A security plan is the plan of action that an organisation intends to use to address its security risk. It is based on the security policy which supports the organisation's goals and resources and a thorough security risk analysis, and is one means to demonstrate a commitment to risk management in general.[8] Information security planning would form an important component of most organisations' overall security plans.

2.17 Organisations did not generally have an overall security plan detailing the level of protection necessary for each category of sensitive information resources and the nature of procedures required to manage the identified risks or the priorities for addressing them.

2.18 For example, most of the organisations had not determined what resources were required for security and the full costs of maintaining security. Many organisations had, however, undertaken a number of

---

[8] Revised PSM, Volume B, paragraph 4.9 refers.

aspects of information security planning, but not coordinated or formalised them in a security plan.

2.19 Organisations were preparing fraud control plans, as required by the *Financial Management and Accountability Act 1997*, but were not giving the same attention to formal security planning.

2.20 The Secretary of the Department of Prime Minister and Cabinet wrote to departmental secretaries and agency heads on 11 July 1997 recommending that each organisation should prepare a Risk Management Plan for IT&T Systems. Responses to this request varied considerably with some organisations providing comprehensive plans and others providing only brief comments. However, none of the organisations examined, had a specific plan already in place that they could call upon to answer the request.

2.21 An additional risk to be considered in today's demanding and technological work environment is away-from-base work, particularly work taken home at the end of the working day. Sensitive information may be taken home in paper form (filed or unfiled) or in electronic form (on portable computer hard disk or on floppy disk for use on home computers). While it was clear that sensitive information was taken home on occasions, most of the organisations had given little consideration to the extent of the practice or to the actual security arrangements that were being applied.

Audit Report No.21, 1997–98

2.22 Recommendation 4 of *Audit Report No.21, 1997–98* recommended that organisations 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.

This recommendation, although aimed at more than information security, would also apply to most organisations in the current audit. Information security aspects of this recommendation are outlined in recommendations 1 and 2 of this report.

Recommendations

Recommendation 1

2.23 The ANAO *recommends* that organisations develop a security risk assessment policy and framework for the whole of their organisation and undertake a security risk assessment in relation to information security (including IT&T). The policy and framework should, among other things, establish the degree of risk that the organisation is prepared to accept and the likely frequency of review and methodology to be used for each assessment. The risk assessment should, among other things:

- identify all information resources;
- identify all the risks to information resources, ie. leaks, theft, sabotage, fraud, as well as the likely perpetrators;
- assess the consequences and likelihood of the risks occurring;
- determine the level of protection that is required for sensitive information; and
- allocate priority for the treatment of the identified risks.

Recommendation 2

2.24 The ANAO *recommends* that, following completion of the risk assessment, organisations develop and implement an integrated security plan to ensure sensitive information is classified and protected on an ongoing basis in accordance with Government requirements and policies specific to the organisation. Such a plan should cover the allocation of responsibility and staff resourcing requirements; the review and maintenance of staff security clearance requirements; the conduct of staff awareness programs; the acquisition of security equipment; an analysis of security controls relating to each of the IT&T systems; and the development, operation and maintenance of monitoring activities (for both paper-based and computer-based information).

2.25 While the above recommendations are focused on information security, they should not be considered in isolation of other security considerations, such as asset security and people security. Accordingly, they should be considered in conjunction with the broader recommendations made in *Audit Report No.21, 1997–98.*

Control environment

2.26 The control environment is critical to the effectiveness of the overall control structure. It impacts on all the other components, providing the foundation for the way organisations conduct their activities

and carry out their responsibilities. It reflects management's commitment and attitude to the implementation and maintenance of an effective control structure. The control environment will influence the design and operation of control policies and procedures and determine their effectiveness in mitigating risks and achieving objectives.

Evaluation criteria

2.27 To achieve an effective control environment over information security it is expected an organisation would have:

- issued policy regarding the objectives and scope of protecting information under the classification system;
- determined responsibilities for managing and accessing the information;
- established physical and technological environments commensurate with the sensitivity of the information maintained;
- developed procedures for policy implementation and treatment of the assessed risks to classified information; and
- promoted the policy, procedures and instructions for classifying and protecting information through staff awareness and training programs.

Overall audit conclusion and main findings

2.28 Most organisations had established a framework for security overall, including the appointment of security officers and establishment of procedures. However, many of them had not given sufficient attention to managing information security in particular. Furthermore, some organisations had not provided the same level of security for IT&T developments as they had for the more traditional aspects of their business operations.

2.29 The main findings in relation to the information security control environment were:

- lack of senior management direction of security operations and limited integration of general security functions with IT&T security functions;
- the non-matching of security clearances with levels of access to sensitive information, and the failure to maintain the currency of clearances;
- the operation of IT&T environments with inadequate security protection levels; and
- insufficient attention to staff awareness and training programs.

Detailed audit findings and recommendations

Responsibility for security

2.30 Historically, organisations have maintained physically secure environments to protect their information and other resources. More recently, they have been confronted with the need to protect an ever-increasing amount of information that is held electronically. At the same time, there has been an increasing emphasis on business operations, together with a need to make information widely available, which has impacted on management's regard for the security function.

2.31 The revised PSM advises that *'a member of the Senior Executive Service, the security executive, should be designated as being responsible for the ongoing development of security policy and the oversight of protective security matters within the organisation'*.[9] It also states that *'each organisation should appoint an agency security adviser (ASA) to be responsible for the day-to-day performance of the protective security function and an information technology security adviser (ITSA) to be responsible for the organisation's electronic communication networks'*.[10] The current PSM also provides for the appointment of the equivalent positions of security executive, ASA and ITSA.

2.32 Most organisations placed responsibility for security at branch head level with the heads of corporate services and information technology generally being assigned the role(s). However, in most instances, security was normally only a small part of the nominated branch head's responsibilities, with day-to-day management being carried out by supporting staff.

2.33 Four of the organisations maintained a security unit of at least two staff within the corporate services area. The other two organisations included security as a part of the duties of a nominated officer (ASA). None of the organisations operated IT&T security units, although most had an officer responsible for IT&T security. The ITSA position of one Category B organisation was left vacant for almost a year while in two of the three Category A organisations there was no designated IT security officer position.

2.34 Most organisations operated IT&T security and general security independently of each other. Consequently, the security policy and procedures for the two areas of responsibility were often developed in isolation of each other, which sometimes led to inconsistencies in the protection of sensitive information resources.

---

[9] Revised PSM (March 1999), Volume A, paragraph 4.9 refers.

[10] ibid

2.35 For example, where paper-based information was required to be stored in a particular class of security container, electronic information was often allowed to be stored on a network without the equivalent level of security.

2.36 Only one of the organisations had some formal integration of the two functions with the IT&T and physical security adviser positions being located together under one manager. Another organisation was attempting to bring policy for the two functions within one section.

2.37 Integration of the two roles in all organisations should provide a more comprehensive approach to, and reporting of, security and related matters (eg. privacy, fraud control). The ANAO therefore considers that the ASA and ITSA positions should be placed under one manager with, as far as is practicable, the latter position being outside of the IT operations area.

2.38 In general, security had a relatively low profile outside of the security units with limited involvement from senior management of the executive and operational areas except where specific problems were identified.

2.39 None of the organisations had a specific operational committee exclusively responsible for security and associated matters. A few of the organisations, however, did have other committees that had an interest in security.

2.40 The ANAO considers, although no longer specifically suggested by the revised PSM, that a security (or other management) committee would be highly desirable, particularly in those organisations that have a wide cross-section of activities dealing with sensitive information. Such a committee would provide an opportunity for operational areas (which generally create and use sensitive information) to participate in the development of policy and assessment of security performance and should lead to the development of a stronger security culture across the organisation.

Audit Report No.21, 1997–98

2.41 *Audit Report No.21, 1997–98* recommended organisations review the allocation of responsibility for security. The recommendation was made 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.

2.42 This recommendation remains just as applicable as it was in December 1997, but takes on greater significance as the 1997–98 audit

did not cover IT&T security. In addition, the need for high level coordination of security needs to be reinforced.

Recommendation 3

2.43 The ANAO *recommends* that organisations:

- integrate the physical and IT&T security functions and responsibilities by, for example, placing the ASA and the ITSA together under one management (and as far as practicable, the ITSA outside of the IT operations branch / section); and
- coordinate the management of all security activities through an appropriate executive responsibility, that is, either enabling an existing management committee or establishing a security committee (or similarly designated committee which may include associated activities eg. privacy), to take responsibility for providing direction and review of security matters (risk assessment, policy, network protection, security cleared positions, integration of security functions, staff awareness program, performance measurement, etc).

Security clearances

2.44 Officers accessing information above the level of 'X-in-Confidence / Restricted' are required to have a current security clearance.

2.45 Clearances may be of two types, Designated Security Assessment Positions (DSAP) or Positions of Trust (POT). A DSAP is a position whose duties involve access to national security information that has been security classified as 'Confidential' or above. A POT is a position whose duties involve access to non-national security information at the level of 'Protected' or above.

2.46 Organisations must determine which positions require occupants to be security cleared and to what level. Government policy is to have the minimum number of people possible subject to security clearances. However, a recent survey of Commonwealth organisations by the PSCC indicated that more than 15 000 clearances are sought in any given year.[11]

2.47 The ANAO found that all of the Category A organisations had a very high proportion of staff with security clearances above the level that their work commitments would normally require. Each organisation had a minimum predetermined clearance level applicable to most staff. While these arrangements are likely to increase the overall level of personnel security within the organisation, they also come at a financial

[11] 1998 survey undertaken by the PSCC as part of a specific review of personnel security procedures. More than half of the clearances were for the Department of Defence.

cost, particularly where officers are unlikely to require access to sensitive information in the normal course of their duties.[12] However, the ANAO acknowledges that there can be operational and administrative efficiencies for an organisation having a predetermined clearance level for staff, eg. where staff are regularly required to move between different positions or organisational areas at short notice, and therefore endorses such arrangements where the benefits clearly outweigh the costs.

2.48 On the other hand, all of the Category B organisations had very few officers cleared, with two of the organisations only recently having become aware of the need for officers to be cleared.

2.49 The ANAO found in each of the Category A organisations, that a number of staff had access to information for which they were not appropriately cleared. The ANAO also found examples of this at two of the Category B organisations. Equally, the ANAO found that several of the cleared staff in most of the organisations did not access sensitive information at the highest level to which they were cleared.

2.50 The need for clearances is complicated by the long processing time, especially where temporary staff and contractors are employed. The processing of a clearance can take over three months to complete. As a result of the long lead time, the ANAO found that officers often obtained access to sensitive information before clearances were obtained (especially where they had just commenced duty in the organisation) or without clearances being initiated (especially in the case of temporary staff). Consequently, there was no guarantee that new or temporary staff were cleared where their work involved classified material or the opportunity to view classified material.

2.51 The ANAO found that one organisation did not allow staff to commence or have an access pass until the clearance process was completed. Under this arrangement staff awaiting clearance needed to be signed into the building each day and, in theory, to be escorted at all times. Another organisation enables temporary access to sensitive information following approval by the security executive in circumstances where officers do not have a current clearance or do not have clearance at the appropriate level. This allows an officer to commence duty while the process of obtaining a clearance is under way and thereby enables the organisation to meet operational needs.

---

[12] The cost of obtaining a Top Secret security clearance through the Australian Security Vetting Service is $1500. Other costs include $900 for a Highly Protected clearance and $600 for a Secret clearance. The Australian Security Vetting Service was established by the Attorney-General's Department in 1996 to undertake security clearances for other Commonwealth organisations on a user-pays basis.

2.52 The failure to ensure that only authorised people have access to sensitive information and the absence of a structured program for ensuring the adequacy of clearance levels increases the risk that sensitive information will be improperly accessed and possibly distributed to unauthorised parties.

2.53 The ANAO considers that more attention needs to be given to the arrangements for determining security clearances for staff handling sensitive information. Organisations need to do this in conjunction with security risk assessments. However, particular organisations may still determine that a high proportion of clearances is necessary.

Reassessment of clearances

2.54 Organisations must periodically reassess a person's suitability to hold a security clearance. At this time, organisations should consider whether there is a continuing need for the clearance, and if so, whether the clearance is at the appropriate level. There are two clearance review procedures—re-validation and re-evaluation.[13]

2.55 For 'Secret' and 'Highly Protected' levels, the May 1999 draft of the revised PSM requires that clearances must be re-evaluated at intervals not exceeding five years. For 'Top Secret' clearances, the minimum requirement is for revalidation every 30 months and a re-evaluation every five years.[14] Similar guidelines exist in the current PSM.

2.56 Most organisations did not maintain the currency of clearances (ie. through revalidations and re-evaluations) in accordance with the requirements recommended in the PSM. Accordingly, a number of officers accessed sensitive information without a current clearance.

2.57 It should be noted that a clearance, in itself, does not guarantee that a person is not a security risk. Management needs to ensure that individual staff with access to sensitive information on an ongoing basis are not only formally reassessed in accord with the PSM requirements, but also observed as to behaviour or circumstances that might require re-assessment at any time.

Management information on security cleared positions

2.58 Organisations need to keep comprehensive and up-to-date personal security files for all employees and contractors who have security clearances.

---

[13] The review processes of re-validation and re-evaluation are described in the Glossary.

[14] Revised PSM, Volume D, Section 8.

2.59 In some organisations, there was no comprehensive database or similar such record which provided up-to-date management information on the security-cleared positions, the occupants of those positions, and the level and currency of each occupant's clearance.

2.60 The ANAO found that the relevant information was generally available in various records, but not sufficiently consolidated to readily enable management recording, reporting and analysis. Where available, full use of the security modules of human resource management systems would enable information on security-cleared positions and personnel to be consolidated and reported in electronic form and thereby enabling up-to-date management reports.

2.61 If organisations regularly monitored staff clearance levels and had their personnel and information management systems linked then the risk of officers gaining access to information for which they were not appropriately cleared would be reduced.

Recommendation 4

2.62 The ANAO *recommends* that organisations:

- as part of the security risk assessment, determine which positions require security clearances and ensure staff occupying those positions have the required level of clearance. This also applies to other personnel who have access to sensitive information or the premises on a regular and an unescorted basis, (eg. contractors, cleaners and maintenance workers); and
- monitor clearance levels at least annually and ensure supervisors are aware of each staff member's clearance level; and provide regular reports on the status of security clearances to the executive (ie. management committee responsible for security, or other similar arrangement).

IT&T environment

2.63 The DSD provides advice and guidance on protective security for IT&T systems. ACSI 33 provides the basic requirements for electronic information security in the Commonwealth. Under the revised PSM, organisations processing or proposing to process national security classified information must consult the DSD.[15]

2.64 The security of the IT&T systems is also dependent on physical security, for which the Australian Security Intelligence Organization (ASIO) is the Commonwealth's advising authority. In this regard, ACSI

[15] Revised PSM, Volume C, paragraph 5.14 refers.

33 outlines requirements relating to security alarms, and ACSI 37 outlines certain other requirements for physical security.

2.65 Computer security was not covered by *Audit Report No. 21, 1997–98*; however, it formed an important element of the current audit.

Certification and accreditation of IT & T systems[16]

2.66 ACSI 33 recommends the certification and accreditation of IT&T systems that are to be used for the processing of sensitive information. Firstly, implementation of the system should be checked and certified by qualified, preferably independent, evaluators, to ensure all technical aspects have been completed in accordance with the planned specifications. Secondly, when all security measures are certified and before the system comes into operation, the system should be accredited to process information up to a specified classification (eg. Secret) by an appropriate accreditation authority. To maintain accreditation, systems should be monitored and the security implications of proposed changes considered by a Configuration Control Board or equivalent.[17]

2.67 Two of the three Category A organisations operated secure networks for the processing of sensitive information above a particular level, in addition to the common networks that were available to all staff. The secure networks at the two organisations had not been accredited by an appropriate accreditation authority. One of the two organisations was currently undergoing accreditation of its networks. In addition, the network operating system at the third organisation had not been certified nor accredited.

2.68 None of the Category B organisations had obtained certification or accreditation of their systems at the time of audit. While this may have been appropriate for their mainframe systems, which only carried sensitive information at the 'X-in-Confidence' level, further consideration of the need to accredit their LAN systems was warranted.

Mainframe v. LAN environment

2.69 The ANAO found that the organisations operating a mainframe environment with high volume transaction processing generally had established a more secure IT&T environment than the organisations operating only a LAN-based environment. It should be noted, however, that the organisations with mainframes, did have some weaknesses in their LAN environments.

---

[16] Certification and accreditation are discussed in the revised PSM Volume C, paragraphs 7.28–7.30.

[17] A Configuration Control Board is a board or management committee which monitors IT&T systems to maintain the systems' accreditation.

Access management controls

2.70 Most of the organisations processed sensitive information on office automation networks that were not secured in accordance with certain recommendations outlined in ACSI 33. All of the organisations exceeded the recommended password expiry period of 30 days with some organisations having no expiry period at all.

2.71 In addition, all six organisations did not conform in relation to at least three of the following security measures:

- recommended minimum number of characters for a password (six characters);
- restrictions on the content of passwords (eg. at least one non-alpha character to be included);
- the maximum number of log-on attempts permitted (three to five attempts); and
- automatic suspension of inactive user accounts.

As a result, organisations were exposed to an increased risk of unauthorised access to sensitive information.

Recommendation 5

2.72 The ANAO *recommends* that organisations:

- review current IT&T networks and applications that process sensitive information, and implement any changes necessary to meet the recommendations outlined in ACSI 33; and
- obtain executive approval for the processing of sensitive information on an IT&T system based on the certification of the system for such purposes by a suitably qualified certification authority.

The development of new networks and applications should also ensure proper security in accordance with ACSI 33. Where the organisations currently process or plan to process sensitive information on electronic systems at the 'Highly Protected' classification level or higher, the organisations should consult ACSI 37 and / or the Defence Signals Directorate.

Staff awareness and training

2.73 The 1991 PSM was aimed mainly at security practitioners while the revised PSM is aimed more generally at managers and staff who need to be aware of the security requirements related to their duties.

2.74 All organisations had distributed some information relating to security. The three Category A organisations had issued comprehensive instructions on a number of aspects relating to security; however, knowledge of the requirements varied among the staff. Staff at the three

Category B organisations had limited awareness of the PSM requirements, but were generally aware of the importance of protecting sensitive information due to various legislative requirements (eg. the Privacy Act and specific legislation administered by the individual organisations).

2.75 Although all six organisations had given some attention to promoting staff security awareness there was no clear strategy in any of the organisations to ensure ongoing information security training and awareness. Furthermore, the ANAO found there was virtually no training in most of the organisations, in relation to the classification system for officers responsible for creating and handling sensitive information, particularly that in electronic form. In the organisations where some training was provided, the training was reasonably basic or not provided to all relevant officers.

Audit Report No.21, 1997–98

2.76 Recommendation 3 of *Audit Report No.21, 1997–98* recommended that organisations[18]:

- 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.

There was little indication that the organisations had devoted more attention to security training and awareness in recent years. At least one organisation had done so, but partly as a response to a security incident.

Recommendation 6

2.77 The ANAO *recommends* that organisations:

- implement a formal staff training and awareness program, which includes, among other things, on-the-job training in the use of the classification system and structured training in IT&T information security; and
- establish a means of assessing the effectiveness of the training and awareness program.

Note: The revised PSM will require compulsory security awareness training for officers (and contractors) who are, or will, access security classified information.

---

[18] Only the parts of the recommendation relating to training and awareness are quoted.

Control measures

2.78 Control measures are the policies and procedures established by management to assist an organisation's achievement of objectives. They are crucial to an effective control structure for treating unacceptable risks and assisting business objectives.

Evaluation criteria

2.79 It is expected an organisation would have implemented control measures relating to:

- classifying information (classification systems);
- restricting access to classified information ('need-to-know' principle); and
- protecting classified information during its life-cycle (procedural controls for the creation, use, maintenance, transmission and disposal of information).

Overall audit conclusion and main findings

2.80 The ANAO concluded that, in many instances, the established control measures for classifying and protecting sensitive information were not well applied or were not as effective as management expected. Furthermore, many staff did not have a detailed understanding of the classification system.

2.81 The ANAO found that non-national security classified material was not generally as well controlled or understood as national security material. This would seem to be a result of the non-national classification levels being relatively new and not being given the same recognition as the national security classified material.

2.82 The main findings in relation to the security control measures were:

- inconsistent interpretation and application of the classification system;
- inconsistent application of protective markings; and
- breakdowns in the storage and transmission of sensitive information resources.

Detailed audit findings and recommendations

Interpretation and application of the classification system

2.83 Security classifications are determined by the degree of harm that may result from the compromise of the information (commonly referred to as the 'harm test'). The determination of classification is largely dependent on the knowledge and experience of the officer classifying

the information. Proper classification requires expertise in the subject matter as well as in the classification system. Further information on the classification system is provided at Appendix 1.

2.84 All organisations incorrectly classified files with over-classification being the most common occurrence. Over-classification has the effect of increasing the costs of protection and restricting the flow of information within the organisation. In addition, there was sensitive material at each of the organisations that had not been classified when it should have been. This material was held in both hardcopy and electronic form. Furthermore, staff normally only classified work that they had created themselves, as there was little indication of classifications being applied to information received from external sources. Finally, documents not placed on official files were not generally classified.

2.85 There was limited understanding of Commonwealth security requirements surrounding the classification of information in the Category B organisations. A common problem among these organisations was the use of the word 'Confidential' for 'X-in-Confidence'. These organisations and to an extent the third parties which they dealt with, used the term 'Confidential' in a general sense rather than its national security sense as outlined in the PSM.

2.86 The level of understanding of the classification system was better in the Category A organisations. Nevertheless, staff generally had difficulty in distinguishing between the classification categories and levels, particularly where all seven levels of classification were in use.

2.87 The ANAO considered that the majority of the breakdowns in the classification of material resulted from staff having insufficient depth of understanding of the classification system. Accordingly, there was scope for identifying specific examples of classified material in the context of each organisation, and for training staff in the application of the classification system.

Recommendation 7

2.88 The ANAO *recommends* that organisations:

- evaluate which documents, forms and data require classification under the requirements of the PSM, and implement procedures to assist in ensuring proper application of the classification system; and
- identify specific examples of classified material in the context of their operations and conduct relevant training in the application of the classification system.

Application of protective markings

2.89 All sensitive documents that require classification under the classification system should be prominently marked with the appropriate security classification (in capital letters, eg. 'PROTECTED', at the centre top and bottom of each page). Electronic documents can be marked using headers and footers, through choosing the appropriate classification when creating a document from a template. Otherwise stamps should be used to mark documents manually.

2.90 The Category A organisations had established templates for the classification of certain electronic documents. Many officers in these organisations and the Category B organisations also inserted header and footers into the documents they created. However, a number of these markings were not particularly prominent (eg. header only, marking at side of page, capitals not used, letters too small). In addition, stamps were not always used in the proper manner. Furthermore, a large number of files in the 'X-in-Confidence' classification were simply marked 'in-confidence' without indicating an appropriate category, eg. 'Audit-in-Confidence', 'Commercial-in-Confidence'.

2.91 In some organisations, particularly those in Category B, large numbers of sensitive documents were not marked with relevant classifications. These included documents such as claim forms, legal documents, material provided by other organisations, and internal forms which deal with information of at least an 'X-in-Confidence' level.

2.92 Where information received requires protection other than that given to it by its originator, the organisation should apply an appropriate Commonwealth classification. However, organisations receiving large amounts of external information did not apply protective markings, but did generally provide extra 'confidentiality' protection through, for example, placing the documents in coloured folders where the choice of colour has a particular significance. Most organisations would find the process of marking large volumes of documents particularly time consuming and resource intensive and would probably be reluctant to apply the PSM requirements. The ANAO considers that each organisation should consider the marking of documents in conjunction with the risks involved and other protective controls in place, eg. physical and personnel security controls. However, where information is provided to other parties, protective markings should always be applied.

2.93 There was no evidence among the papers examined of time-limited protective markings. No organisation seemed to have given any consideration to such classifications, despite a common view from many respondents that much of the information was only sensitive for short

time periods prior to becoming public. In addition, there was no evidence of paragraphs being marked to indicate the sensitive material within a classified document where the majority of the material within the document was not sensitive or where the level of sensitivity varied.

Recommendation 8

2.94 The ANAO *recommends* that organisations:

- develop electronic document templates which include the protective markings as headers and footers;
- encourage the use of time-limited classifications; and
- ensure that sensitive documents received from other organisations or individuals are marked with the relevant Commonwealth classification on all pages.

Storage and transmission of sensitive information

2.95 The PSM outlines the requirements that organisations need to meet in order to achieve specifically designated levels of physical security[19]. Premises may be deemed 'secure', 'partially secure' or 'intruder resistant' depending on the security provided. The requirements for physical protection of sensitive information (in terms of types of security containers) are less stringent within a secure building than in an intruder resistant building.

2.96 Although not specifically examined in this audit, the ANAO observed that organisations were generally very aware of the overall physical security arrangements that had been established for each of their buildings. However, the PSM security requirements were not always consistently applied within the organisations. For example, paper and electronic files were often exposed to unauthorised access because of various breakdowns in the protection of information in use or in transmission.

2.97 The more common breakdowns were:

- files not being locked away during lunch times and other periods of absence or overnight;
- files being stored in cabinets below the minimum storage requirements and cabinets left unlocked;
- sensitive information stored on insecure electronic networks and computers left on without the protection of screen saver passwords; and
- delays in amending staff access to IT&T networks following staff movements and the absence of access reviews on a regular basis.

---

[19] Physical security requirements are outlined in Volume E of the revised PSM.

2.98 In the three Category A organisations staff interviewed were generally conscious of the 'need-to-know' principle and aware of the storage requirements for classified material. However, there was a relatively high number of physical security breaches recorded each month, together with some weaknesses in the protection of electronic information including the inappropriate storage of sensitive material on IT&T systems. Instances were also noted where classified documents were transmitted as email attachments, also posing the risk of unauthorised access. A clear desk policy was in place at each of these organisations and the majority of breaches recorded related to containers being left insecure overnight and keys and/or files being left out.

2.99 Category B organisations were aware of the 'need-to-know' principle but did not have an effective clear desk policy and had several cases where the storage requirements of the PSM were not complied with.

Recommendation 9

2.100 The ANAO *recommends* that organisations:

- reassess the adequacy of requirements and facilities for storage and transmission of sensitive information in terms of the PSM;
- implement a clear desk policy to encourage the protection of sensitive information;
- ensure staff have access to appropriate physical and electronic facilities for storing and transmitting sensitive information; and
- require screen saver passwords to be used on all computer workstations.

Monitoring and review processes

2.101 Monitoring and review is the final component of an effective control structure. Management needs to monitor and review its operations to ensure that program objectives and control activities are being achieved efficiently and effectively. In addition to performance monitoring, the effectiveness of the control structure itself also needs to be monitored and reviewed. Control monitoring and review can be undertaken in two ways, by ongoing monitoring and by separate reviews and evaluations.

Evaluation criteria

2.102 An organisation would have regular monitoring and review processes to ensure classification policies and procedures are adhered to and properly applied, and to identify changes and weaknesses in the

security environment. Such a framework should cover physical inspections, the monitoring of audit trails and reporting of performance to appropriate levels of management, and be closely linked with the risk assessment process discussed earlier.

Overall audit conclusion and main findings

2.103 The ANAO concluded that most of the organisations needed to devote more attention to the monitoring and reporting processes. Four of the six organisations conducted physical after-hours inspections on a regular basis and detected a relatively high level of security breaches. However, only one organisation regularly monitored the IT&T audit monitoring logs.

Detailed audit findings and recommendations

Physical monitoring

2.104 Each of the Category A organisations conducted a regular after-hours inspection program to ensure compliance with physical security procedures overnight. The inspecting officers secured any unprotected classified containers or information and recorded details of the security breaches observed. The checks concentrated on unsecured security containers, opened key safes and exposed files and documents, but did not include papers in other types of containers eg. closed desk drawers or papers covered up on desks. Furthermore, two of the three organisations did not include logged-on computers in the reported breaches.

2.105 The ANAO found that the number of physical security breaches reported as a result of overnight monitoring in the Category A organisations had remained at a relatively high level during 1998. However, one of these organisations had shown a marked improvement on recent years. Nevertheless, the level of breaches highlights the need to improve security compliance/awareness relating to the protection of sensitive information.

2.106 Two of the three Category B organisations did not have regular formal after-hours inspection programs to monitor staff compliance with security requirements and address issues relating to the security of classified material. While the third organisation did conduct a daily check of security containers, no records of the breaches detected were kept for a period of 12 months prior to the audit commencing.

2.107 As a result, management was unaware of the level of security compliance/awareness at each of the Category B organisations.

2.108 None of the organisations carried out security checks during the day, at a time when information is widely available to all persons within the building. The ANAO considers that the risk of unauthorised access is likely to be higher during business hours, especially during lunch times and other similar periods of absence.

IT&T monitoring

2.109 There was less IT&T monitoring than physical monitoring. There was a lack of audit trail recording in some organisations and a lack of monitoring in most organisations. Specific matters included inadequate review of inactive user accounts and system administrator activity. Failure to monitor the logs for such events exposes the risk that unsuccessful attempts may, if given the time that lack of detection provides, become successful, and lead to unauthorised access to information.

2.110 There was no monitoring of the information stored on networks to detect classified information above the levels for which the networks were suitable. Furthermore, there was no monitoring of the quantity of classified information maintained.

Reclassification of files

2.111 There was also no established program for reviewing the classification of files. In addition, where re-classifications did occur, no records were maintained. Such records would provide information on the reliability of file classifications and the effectiveness of procedures.

Reporting

2.112 The Category A organisations reported physical security breaches to senior management on a regular basis. Generally, however, there was no other regular reporting on security activities or performance.

2.113 Until recently, none of the organisations had implemented stringent procedures for dealing with the officers found to be responsible for security breaches. One organisation was now considering the number of security breaches in assessing the performance of individual officers.

Audit Report No.21, 1997–98

2.114 Recommendation 5 of *Audit Report No.21, 1997–98* recommended that organisations:

- 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.

This recommendation was principally aimed at the recording and reporting of security incidents. However, as found in the current audit, there is a need for organisations to establish programs to detect potential security incidents in relation to sensitive information.

Recommendation 10

2.115 The ANAO *recommends* that organisations develop a formal security monitoring and review program, incorporating both physical and IT&T security aspects. The program should be utilised to analyse areas of security weaknesses, highlight procedural deficiencies and/or identify where the policies and practices require revision. Such a program could include periodic after-hours inspections, regular reviews of all IT&T system audit trails, periodic electronic searches of departmental LANs and personal computer hard drives, and periodic examination of file classifications. Organisations should also develop clear procedures for dealing with offenders. This could involve various internal disciplinary measures and incorporating breach incidents as a performance measure in performance agreements.

Canberra ACT
11 August 1999

P. J. Barrett
Auditor-General

Appendices

Glossary

agency security adviser (ASA) the person nominated by the agency for the day-to-day performance of the protective security function within the agency.

agency security plan the plan of action the agency intends to use to address its security risk based on the context in which an agency operates and a thorough risk review. It is one of the means by which an agency will demonstrate a commitment to general risk management.

clear desk policy a policy which dictates that people must ensure that security classified material and other valuable resources are secured appropriately when absent from the work place.

classification system—there are seven levels of classification: four national security (Restricted, Confidential, Secret and Top Secret) and three non-national security (X-in-Confidence, Protected and Highly Protected). The non-national security classifications of 'Protected' and 'Highly Protected' only came into existence in 1990. Details on how to classify information are at Appendix 1.

confidentiality (of information) the limiting of official information to authorised users for approved purposes. The confidentiality requirement is determined by reference to the likely consequences of unauthorised disclosure of official information. The Commonwealth's security classification system has been developed to help agencies identify information that has confidentiality requirements.

Configuration Control Board a board (whose membership must always include the ASA) which monitors IT systems to maintain the systems' accreditation.

Designated Security Assessment Position (DSAP) a position whose duties involve access to national security information that has been security classified as 'Confidential' or above.

encryption the process, which may be irreversible, of transforming data into an unintelligible form.

harm any negative consequence, such as compromise of, or damage to, or loss incurred by, the Commonwealth.

information/information resources in the context of the PSM, this includes documents and papers; electronic data; the software or systems and networks on which the information is stored, processed or communicated; intellectual information acquired by individuals; and physical items from which information regarding design, components or use could be derived.

information security a procedural system implemented to ensure that official information is protected from compromise or misuse.

information technology security adviser (ITSA) a person nominated by the agency head to provide advice on information technology-related security issues within his or her agency.

intruder resistant area an area secured so that it is suitable for handling, storing and processing security classified material up to and including 'Secret'.

IT&T information technology and telecommunications.

national security a term used to describe the safety of the nation from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference.

national security information official information whose compromise could affect the security of the nation (for example, its defence or its international relations). National security information could be about security from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference; defence plans and operations; international relations; and national interest (economic, scientific or technological matters vital to Australia's stability and integrity).

'need-to-know' principle the principle that the availability of official information should be limited to those who need to use or access the information to do their work.

non-national security information official information whose compromise does not threaten the security of the nation but could threaten the security or interests of individuals, groups, commercial entities, government business and interests, or the safety of the community. Examples of this type of information include information on law enforcement operations and personal information pertaining to members of the public.

partially secure area an area suitable for processing, storing and handling security classified information up to and including 'Top Secret'. A partially secure area is more secure than an intruder resistant area, but less secure than a secure area.

personal information information or an opinion (including information forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identify is apparent, or can reasonably be ascertained, from the information or opinion.

personnel security a procedural system implemented to ensure that only those people whose work responsibilities require them to access official information and official resources have such access. This is done by limiting the number of people who have access to those who can demonstrate a need to know and whose eligibility had been determined after a comprehensive evaluation of their history, attitudes, values and behaviour.

physical security the part of protective security concerned with the provision and maintenance of a safe and secure environment for the protection of agency employees and clients, and physical measures designed to prevent unauthorised access to official resources and to detect and respond to intruders.

Position of Trust (POT) a person whose duties involve access to non-national security information to the level of 'Protected' and above.

protective marking an administrative label assigned to security classified information which not only shows the value of the information but also tells users that the information has been security classified; what level of protection must be provided during use, storage, transmission, transfer and disposal; and whether the information is national security or non-national security. The protective marking must be in capitals, bold text, and or a minimum height of 5 mm. Examples of protective markings are: 'Top Secret, Secret, Confidential, Restricted, Highly Protected, Protected, In-Confidence'.

protective security the total concept of information, personnel, physical and information technology and telecommunications security.

re-evaluation (of personnel security clearance) the process of reviewing a previously cleared officer and making a reassessment about his or her suitability for the clearance; it includes a new police check and the provision of names of five referees by the officer.

re-validation (of personnel security clearance) a type of security clearance review procedures which is essentially an interim check to ensure that the previously cleared officer has not experienced any relevant change of circumstances and that no security concerns have arisen in the workplace; it involves seeking information from the officer and his or her supervisor but does not involve referees or police checks.

risk exposure to an event which could result in loss or harm. Risk is measured in terms of vulnerability, event likelihood and event consequence.

risk management the systematic application of management policies, procedures and practices to the tasks of identifying, analysing, evaluating, treating and monitoring risk.

secure area an area secured so that it is suitable for handling, storing and processing security classified information up to and including either 'Secret' or 'Top Secret'.

security breach an accidental or unintentional failure to observe the requirements for handling official resources.

security executive the agency Senior Executive Service officer (or equivalent) responsible for protective security functions in that agency.

security incident a security breach, violation, contact or approach from those seeking unauthorised access to official resources, or any other occurrence which results in negative consequences for the Commonwealth.

security risk a measure of potential loss or harm relevant to an agency's protective security arrangements.

security risk review the process used to determine risk management priorities by evaluating risk adjacent predetermined criteria, in the context of an agency's protective security arrangements.

threat assessment evaluation and assessment of the intentions of people who could pose a hazard to a resource or function, how they might cause harm and their ability to carry out their intentions. Threats must be assessed to determine what potential exists for them to actually cause harm.

unauthorised access (to information) access to official information which is not based on a legitimate need to know, sanctioned by government policy or agency direction, or an entitlement under legislation.

unauthorised disclosure (of official information) the communication or publication of official information where it is not based on a legitimate need to know, sanctioned by government policy or agency direction, or an entitlement under legislation.

Appendix 1

Classification System—How to classify information

The classification system for sensitive information in the Commonwealth is divided into two categories of information, namely, national security information (eg. defence and international relations) and non-national security information (eg. commercial and personal). The national security classifications comprise TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED while the non-national security classifications are HIGHLY PROTECTED, PROTECTED and X-IN-CONFIDENCE. The national security classifications are long standing and are used by other countries. The first two mentioned non-national security classifications were introduced in 1990.

The remainder of this appendix comprises an extract from the revised PSM and a flow chart outlining how the various classification levels should be used (the 'Harm Test').

Extract from Section 6 Volume C of the revised PSM (March 1999 edition)

How to identify national security information

6.22 National security information is any official resource (including equipment) that records information about or is associated with Australia's:

- **security** from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference
- **defence** plans and operations
- **international relations**, which relate to significant political and economic relations with international organisations and foreign governments
- **national interest**, which relates to economic, scientific or technological maters vital to Australia's stability and integrity.

6.23 **Not all information about these matters needs to be security classified. This information must only be security classified if its compromise could damage national security.**

How to identify non-national security information

6.24 Non-national security information is any official resource (including equipment) that requires increased protection and does not meet the definition of national security information. Most often this will be information about:

- **government or agency business**, whose compromise could affect the government's capacity to make decisions or operate, the public's confidence in government, the stability of the market place and so on
- **commercial interest**, whose compromise could affect the competitive process and provide the opportunity for unfair advantage
- **law enforcement operations**, whose compromise could hamper or render useless crime prevention strategies or particular investigations or adversely affect personal safety
- **personal** information, which is required to be protected under the provisions of the Privacy Act, the Archives Act, or other legislation.

6.25 Not all information about these matters needs to be security classified. This information must only be security classified if the compromise could cause damage.

How to assign protective markings to national security information

6.29 There are four levels of national security protective markings. These markings reflect the **consequences** of the compromise of the information.

RESTRICTED

6.30 The **RESTRICTED** marking should be used when the compromise of the information could cause **limited damage** to national security. For instance:

- adversely affect diplomatic relations
- hinder the operational effectiveness or security of Australian or allied forces
- adversely affect the internal stability of Australia or other countries.

CONFIDENTIAL

6.31 The **CONFIDENTIAL** marking should be used when the compromise of the information could cause **damage** to national security. For instance:

- damage diplomatic relations (that is, cause formal protest or other sanction)
- damage the operational effectiveness or security of Australian or allied forces
- damage the effectiveness of valuable security or intelligence operations
- disrupt significant national infrastructure
- damage the internal stability of Australia or other countries.

6.32 Most national security information would be adequately protected by the procedures given to information marked CONFIDENTIAL or RESTRICTED.

SECRET

6.33 The **SECRET** marking should be used when the compromise of the information could cause **serious damage** to national security. For instance, compromise could:

- raise international tension
- seriously damage relations with other governments
- seriously damage the operational effectiveness or security of Australian or allied forces
- seriously damage the continuing effectiveness of highly valuable security or intelligence operations
- shut down or substantially disrupt significant national infrastructure
- seriously damage the internal stability of Australia or other countries.

This marking should only be used sparingly.

TOP SECRET

6.34 The **TOP SECRET** marking requires the **highest degree** of protection as the compromise of the information could cause **exceptionally grave damage** to national security. For instance, compromise could:

- threaten directly the internal stability of Australia or other countries
- lead directly to widespread loss of life
- cause exceptionally grave damage to the effectiveness or security of Australian or allied forces
- cause exceptionally grave damage to the effectiveness of extremely valuable security or intelligence operations
- cause exceptionally grave damage to relations with other governments
- cause severe long-term damage to the Australian economy.

Very little information warrants this marking, which is to be used with the utmost restraint.

How to assign protective markings to non-national security information

6.35 There are three levels of non-national security protective markings which indicate the level of protection to be given to non-national security classified information. As with national security information, these markings reflect the **consequences** of the compromise of the information.

X-IN-CONFIDENCE

6.36 The **X-IN-CONFIDENCE** marking is used when the compromise of the information could cause **limited damage** to the Commonwealth, the Government, commercial entities or members of the public. This protective marking is accompanied by a notification of the subject matter to ensure correct handling and an easy appreciation of the need-to-know requirement. When the PSM refers to this type of information, the marking appears as X-IN-CONFIDENCE.

6.37 Examples of types of X-CONFIDENCE markings include STAFF-IN-CONFIDENCE, SECURITY-IN-CONFIDENCE, COMMERCIAL-IN-CONFIDENCE, AUDIT-IN-CONFIDENCE.

6.38 **Note that the X-IN-CONFIDENCE marker does not include Cabinet-in-Confidence information (see paragraphs 6.64–6.66).**

6.39 Information that might be classified as X-IN-CONFIDENCE includes information whose compromise could:

- cause substantial distress to individuals or private entities
- cause financial loss or loss of earning potential to, or facilitate improper gain or advance for, individuals or private entities
- prejudice the investigation or facilitate the commission of crime
- breach proper undertakings to maintain the confidentiality of information provided by third parties
- impede the effective development or operation of government policies
- breach statutory restrictions on the management and disclosure of information
- disadvantage the Government in commercial or policy negotiations with others
- undermine the proper management of the public sector and its operations.

PROTECTED

6.40 The **PROTECTED** marking is used when the compromise of the information could cause **damage** to the Commonwealth, the Government, commercial entities or members of the public. For instance, compromise could:

- endanger individuals and private entities
- work substantially against national finances or economic and commercial interests
- substantially undermine the financial viability of major organisations
- impede the investigation or facilitate the commission of serious crime
- seriously impede the development or operation of major government policies.

6.41 Most non-national security information would be adequately protected by the procedures given to the information marked X-IN-CONFIDENCE or PROTECTED.

HIGHLY PROTECTED

6.42 The **HIGHLY PROTECTED** marking indicates that the information requires a **substantial degree** of protection as compromise of the information could cause **serious damage** to the Commonwealth, the Government, commercial entities or members of the public. For instance, compromise could:

- threaten life directly
- seriously prejudice public order
- substantially damage national finances or economic and commercial interests.

6.43 Very little information belongs in the HIGHLY PROTECTED category and the marking should be used sparingly.

Cabinet documents

6.64 Documents used by Cabinet to formulate policy and make decisions require special protective measures. These measures are detailed in Chapter 9 of the *Cabinet Handbook*, February 1994.

Classifying and marking Cabinet documents

6.65 All documents prepared for consideration by Cabinet, including those in preparation, are to be marked Cabinet-in-Confidence, regardless of any other security consideration. This is because Cabinet documents, unlike other official information, belong to the governments that create them. They are integral to the process by which governments make decisions and they constitute the record of these decisions. Any unauthorised disclosure of them damages the openness and frankness of discussions in the Cabinet Room and thereby impedes the process of good government. Therefore, the *Cabinet Handbook* stipulates that the minimum level of protection given to Cabinet documents is to be equivalent to information marked as PROTECTED. It follows that the minimum clearance for access to Cabinet information is PROTECTED. Cabinet material is always accountable material (see paragraphs 7.16–7.17).

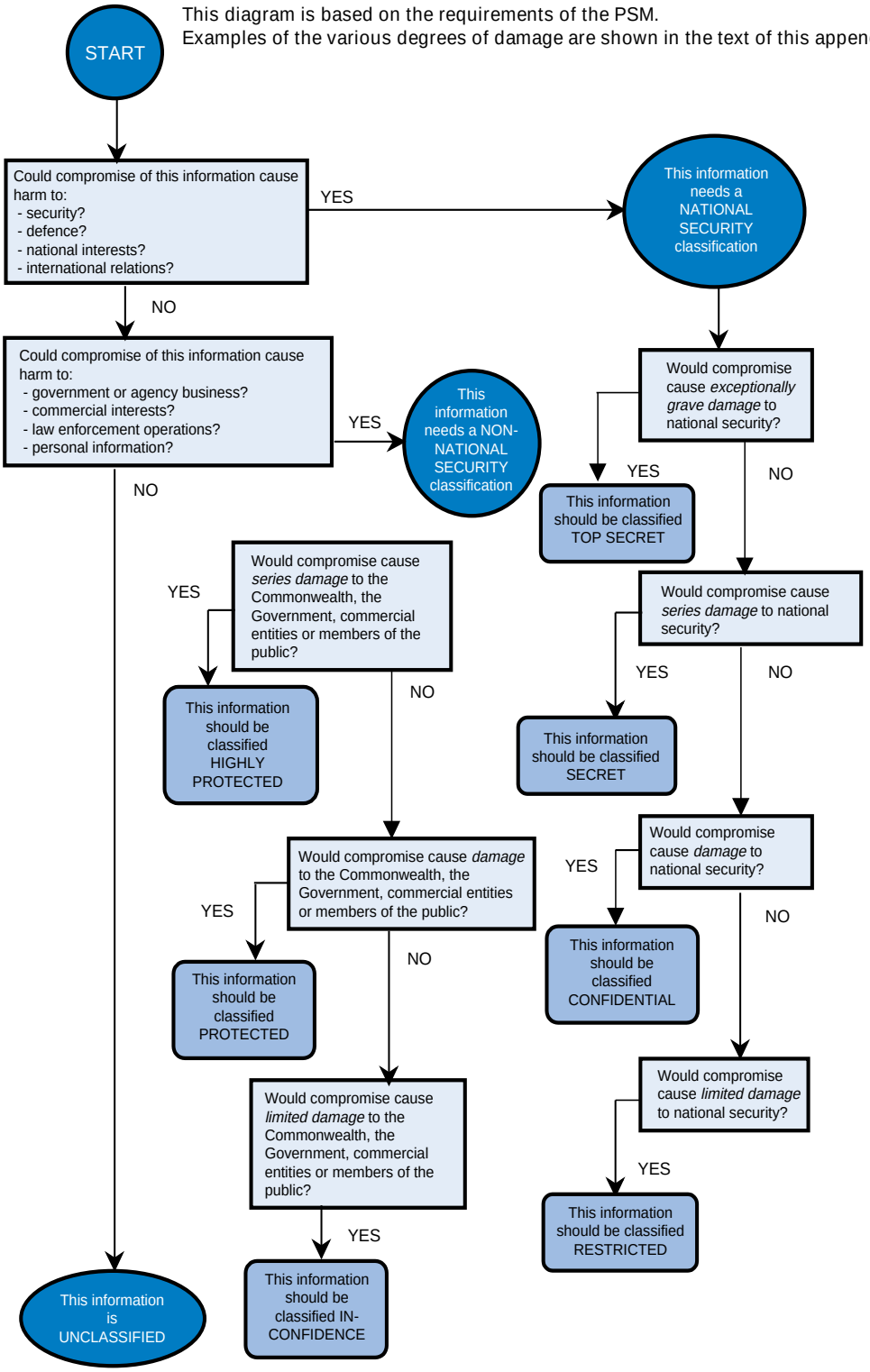
6.66 Cabinet documents can require a higher level of protection, depending on their subject matter. In this case, the Cabinet document must show, immediately after the Cabinet-in-Confidence marker, either the HIGHLY PROTECTED marker, if the matter is non-nation security, or one of the higher national security protective markings. For instance: Cabinet-in-Confidence-SECRET.

A flow chart on **'How to select an appropriate security classification'** follows.

Figure 1

How to select an appropriate security classification

This diagram is based on the requirements of the PSM.
Examples of the various degrees of damage are shown in the text of this appendix.



Appendix 2

Unauthorised disclosures between March 1996 and October 1998 as reported in Australian Senate Hansard

The information shown in this appendix is based upon questions asked in December 1998.

Departments	*Q.1*	*Q.2*	*Q.3*
Agriculture, Fisheries and Forestry	0	N/a	N/a
Attorney-General	2	Yes	No
Communications, Information Technology and the Arts	1	Yes	No
Defence	2	Yes	No
Education, Training and Youth Affairs	1	Yes	No
Employment Workplace Relations and Small Business	1	No	No
Environment and Heritage	6	Yes	No
Family & Community Services *(a)*	20	Yes	No
Finance and Administration	1	Yes	No
Foreign Affairs and Trade (DFAT) *(b)*	-	-	-
Health and Aged Care	1	Yes	No
Immigration and Multicultural Affairs (DIMA) *(c)*	15	9	3
Industry, Science and Resources	1	Yes	No
Prime Minister and Cabinet	5	Yes	No
Transport and Regional Services	0	N/a	N/a
Treasury	0	N/a	N/a
TOTAL	**56**	**49**	**3**

Q.1 On how many occasions did the department refer unauthorised disclosures to the Australian Federal Police (AFP) between March 1996 and October 1998?

Q.2 In each instance where an investigation has been undertaken has that investigation been concluded?

Q.3 Have any officers been charged with offences relating to unauthorised disclosures that occurred during this period, if so, how many?

Notes:

(a) (Q.1)—Very few privacy/confidentiality allegations are referred to the Australian Federal Police for investigation as Centrelink officers have the skills and resources to effectively investigate the majority of allegations. Centrelink officers refer substantiated cases directly to the Director of Public Prosecution for consideration of prosecution action. The majority of cases referred to the Australian Federal Police for investigation are cases involving unauthorised access to Commonwealth information and attempted soliciting of information. During the 1995 to 1998 financial years a total of 20 cases of privacy/confidentiality allegation were referred to the Australian Federal Police for investigation.

(Q.2)—No cases of unauthorised disclosures are under investigation by the Australian Federal Police.

(Q.3)—During the 1995 to 1998 financial years there were no departmental or Centrelink officers charged by the AFP with offences relating to unauthorised disclosure of information.

(b) In order not to prejudice the efforts of police & other authorities in current and future investigations into unauthorised disclosures of information, the Government does not propose to reveal details of cases that have been or are under investigation, or the number of cases involved. Further, the Government does not propose to confirm whether or not individual disclosures reported in the press were unauthorised.

(c) (Q.1)—DIMA did not refer any unauthorised disclosures to the Australian Federal Police between March 1996 and October 1998. During this period 15 allegations were referred to the Department's Internal Investigations Section (IIS) for investigation. Officers of the IIS are qualified to conduct criminal investigations on behalf of the Department.

(Q.2)—Nine have been concluded and six remain under investigation.

(Q.3)—Three officers have been charged with offences relating to unauthorised disclosures during this period.

Appendix 3

Summary of Audit Report No.21, 1997–98, *Protective Security* [20]

Introduction

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

Within the Commonwealth each organisation is responsible for establishing protective security arrangements commensurate with its operational responsibilities and environment. The Attorney-General's Department is responsible for the development and coordination of protective security policy, and issues standards and guidelines in the form of a Commonwealth protective security manual.

Audit objectives

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

The audit did not include computer security and communications security.

Audit conclusion and key findings

The ANAO found that most organisations 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 organisations; and, as a result, the potential for breaches of security was sometimes higher than would normally be desirable. The ANAO concluded that there is a need to raise the profile of security management and awareness across Commonwealth organisations.

In addition, there had been a need for some time for the Commonwealth protective security manual to be updated as a result of changes in the

---

[20] *Audit Report No.21, 1997-98, Protective Security* was tabled in Parliament on 5 December 1997.

public sector and security environments over recent years, eg. outsourcing, and increasing reliance on information technology systems. The Attorney-General's Department had issued an exposure draft of a new protective security manual in December 1997. At that time, the Department anticipated that the revised manual would be issued during 1998.[21]

The key audit findings were:

- insufficient allocation of responsibility and accountability for protective security to program level;
- limited security training for staff, including security officers;
- risk reviews not updated for changes in the security environment;
- lack of formal planning detailing the treatment of identified risks;
- 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
- inadequacies in the monitoring of security incidents, and in the review of automated recording systems.

Better practice

Better practice principles and guidelines were included as an appendix to the report. The principles and guidelines were largely based on the revised draft of the protective security manual.

Recommendations

The ANAO made five recommendations, one for the Protective Security Policy Committee, and four for all Commonwealth organisations to consider. The recommendations for all organisations are repeated below.[22]

Recommendation 2

—that organisations 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.

---

[21] The revised PSM is now expected to be issued in 1999.

[22] Each of these recommendations was considered in the audit of the *Operation of the Classification System for Protecting Sensitive Information*.

Recommendation 3

—that organisations:

- 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.

Recommendation 4

—that organisations 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.

Recommendation 5

—that organisations:

- 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.

Appendix 4

Audit background, objectives, criteria and approach

Protecting information

Information is a major resource of most organisations, and accordingly, its protection is of paramount importance. In this context, information includes documents and papers; electronic data; software, systems and networks; intellectual property/knowledge; and physical items from which information regarding design, components or use could be derived.

Information security comprises three basic components, namely[23]:

- *confidentiality*—protecting sensitive information from unauthorised disclosure or intelligible interception;
- *integrity*—safeguarding the accuracy and completeness of information and computer software; and
- *availability*—ensuring that information and vital services are available to users when required.

This audit is concerned with *protecting sensitive information*, that is, the *confidentiality* component of information security.

Commonwealth policy

Commonwealth policy in relation to information security is contained in the Commonwealth Protective Security Manual (PSM) issued by the Attorney-General's Department. The relevant parts of the current (1991) PSM are Part III 'Administrative and Procedural Arrangements' and Part VI 'Computer and Communications Security'. However, an exposure draft of a revised PSM was issued in late 1997 and a new version of the PSM is expected to be released shortly. The exposure draft consists of eight volumes, Volume C being titled *Information Security*.[24] Volume C is supplemented, in relation to information technology and telecommunications (IT&T) security by the Defence Signals Directorate (DSD) publications, in particular Australian Communications-Electronics Security Instructions (ACSI), ASCI 33 and 37.

---

[23] Australian / New Zealand Standard AS/NZS 4444:1996 *Information security management.*

[24] The current manual was first published in January 1991; a revised manual is expected to be published in 1999.

Classification system

The Commonwealth operates on the basis that information should be *classified* according to a *classification system,* where the *compromise* of such information *could cause harm* to the nation, public interest, the government or other entities or individuals. Information of this type is commonly referred to as *sensitive information.*

The classification system for sensitive information in the Commonwealth is divided into two categories of information, namely, national security information (eg. defence and international relations) and non-national security information (eg. commercial and personal). The national security classifications comprise TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED while the non-national security classifications are HIGHLY PROTECTED, PROTECTED and X-IN-CONFIDENCE. The national security classifications are long standing and are used by other countries. The first two mentioned non-national security classifications were introduced in 1990. Further details of the classification system are provided in Appendix 1.

Previous audit coverage

The ANAO completed two audits on security matters across a range of organisations during 1997–98.

Audit Report No. 21, 1997–98, Protective Security

Audit Report No. 21, 1997–98, Protective Security, reviewed, among other things, information security other than computer and communications security, against the policy and procedures outlined in the 1991 PSM. That audit found inconsistencies in the identification and marking of classified information and weaknesses in the handling and storage of classified information. A summary of Audit Report No. 21, 1997–98, including each of the across-the-board recommendations provided at Appendix 3.

Audit Report No. 15, 1997–98, Internet Security Management

Audit Report No. 15, 1997–98 Internet Security Management examined policies, access control and user education in relation to the use of the Internet; it found a lack of planning relating to policy and procedures and risk assessments and a some need for improved controls.

Other public review

'In Confidence'

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.

Privacy Commissioner

The Privacy Commissioner conducts audits of Commonwealth organisations 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.

Audit objectives and scope

The audit was the first of a series of specific selected topics designed to follow on from the broad coverage of *Audit Report No. 21, 1997–98, Protective Security.*

The main objectives of the audit were:

- to determine whether organisations are *protecting the confidentiality of sensitive information* in accordance with the Commonwealth's security classification system, related Government policy, standards and guidelines, and recognised best practice; and
- to recommend improvements as necessary.

The audit scope was restricted to the *confidentiality* requirements of the Commonwealth's information security classification system. The main focus of the audit was on the identification of material requiring protection and on the administrative security arrangements and controls for protecting classified paper-based and computer-based information. Some aspects of physical and personnel security were also necessarily examined as there is a close relationship between information, physical and personnel security. Audit procedures were based on various volumes of the proposed revised PSM (especially Volume C) and on ACSI 33 and 37 (in relation to IT&T systems), as well as the current PSM.

The audit did *not* attempt to provide an opinion on the overall security of the organisations examined. Furthermore, the audit did *not* cover voice communications, and IT&T systems were *not* examined in relation to the integrity and availability components of information security.

About the organisations

The audit was undertaken at six organisations. The organisations held a range of sensitive information. They ranged in size from 300 to more than 3000 staff and included centrally based and widely distributed organisations. Most of them had significant IT&T operations. Regional offices were examined at two of the organisations.

The organisations fitted into two different categories, with three organisations in each category. The categories were:

- those with a range of national security and non-national security information at all classification levels (hereafter referred to as Category A organisations); and
- those with a significant proportion of low level non-national security information (ie. 'X-in-Confidence' information) and small amounts of classified information at higher levels (hereafter referred to as Category B organisations).

None of the organisations was covered by the previous audits. Due to the nature of protective security arrangements, the organisations are not named in this report.

Audit criteria

The operation of the security classification system was assessed against the following audit criteria:

- *security risk assessment and planning*—organisations would be expected to have determined which information resources require protection under the classification system and to have developed an information security plan, following an assessment of the value of all information resources and the likely risks to those resources; this would normally be done through the conduct of risk assessments (Volume B of the revised PSM refers);
- *security control environment*—organisations would be expected to have issued policy regarding the objectives and scope of protecting information under the classification system, determined responsibilities for managing and accessing the information, established physical and technological environments commensurate with the sensitivity of the information maintained, developed procedures for policy implementation and treatment of the assessed risks to classified information, and promoted the policy, procedures and instructions for classifying and protecting information through staff awareness and training programs (Volumes A, B and C of the revised PSM refer);
- *security classification control measures*—organisations would be expected to have operational programs and systems for classifying information (classification systems), restricting access to that information ('need to know' principle); and protecting that information during its life-cycle (procedural controls for the creation, use, maintenance, transmission and disposal of information)—(Volumes C, D and E of the revised PSM refer); and
- *security monitoring and review processes*—organisations would be expected to have regular monitoring and review processes to ensure that classification policies and procedures are adhered to and properly applied, and to identify changes and weaknesses in the security environment (Volumes A and C of the revised PSM refer).

Audit approach and coverage

The audit was conducted in accordance with ANAO Auditing Standards and was undertaken in the period October 1998 to April 1999. The main elements of the audit approach were:

- development of a comprehensive plan based on the requirements of the PSM and ACSI 33 and good management practices;
- selection of organisations suitable for the review (excluding those organisations examined in the protective security audits of 1997–98);
- completion of field work in accord with the plan at the six organisations finally selected for review;
- analysis of organisation policies, practices and processes;
- liaison with the Attorney-General's Department in relation to security policy and training;
- the issue of a report to each of the six organisations highlighting the practices observed and proposing recommendations for improvement; and
- the issuing of reports to the relevant Ministers.

The ANAO conducted the audit at each organisation within the areas of the security function and information management (including information technology operations), as well as at a selection of policy / operational areas (where information is created and actioned).

The audit process involved interviews with selected officers, the examination of security management and policy / operational files and records, the use of computer software to assist with the review of information technology security, and general observation and inspection.

Each of the organisations was issued with a comprehensive report comprising an executive summary and detailed report outlining the audit conclusions, findings and recommendations applicable to each organisation. The organisations received the audit reports in a cooperative manner and responded to the individual recommendations in a positive manner. The ANAO considers that implementation of the recommendations will lead to improved information security.

Performance information

The reports to the organisations examined included a total of 110 recommendation (ie. an average of 18 per organisation). Of the recommendations, 103 (94 per cent) were agreed or agreed with qualification.

The recommendations were mainly aimed at improving security performance and compliance, and accordingly, did not identify any quantifiable savings. Nevertheless, implementation of the recommendations should result in qualitative improvements in the protection of sensitive information.

The cost of the audit was $560 000. The average cost of the field work undertaken at each of the six organisations was $69 700. Planning and reporting costs amounted to $141 800.

Appendix 5

Revised Protective Security Manual[25]

The revised Protective Security Manual (PSM) consists of eight volumes as follows:

Volume	Title
A	Protective Security Policy
B	Guidelines on Managing Security Risk
C	Information Security
D	Personnel Security
E	Physical Security
F	Security Framework for Competitive tendering and Contracting (CTC)
G	Guidelines on Security Incidents and Investigations
H	Security Guidelines on Home-based Work

[25] The revised manual is expected to be released in 1999.

Index

Series Titles

Titles published during the financial year 1999–2000

Audit Report No.1 Performance Audit
Implementing Purchaser/Provider Arrangements between Department of Health and Aged Care and Centrelink
Department of Health and Aged Care
Centrelink

Audit Report No.2 Financial Control and Administration Audit
Use of Financial Information in Management Reports

Audit Report No.3 Performance Audit
Electronic Travel Authority
Department of Immigration and Multicultural Affairs

Audit Report No.4 Performance Audit
Fraud Control Arrangements in Education, Employment, Training and Youth Affairs

Better Practice Guides

Administration of Grants	May 1997
AMODEL Illustrative Financial Statements 1998	Jul 1998
Asset Management	Jun 1996
Asset Management Handbook	Jun 1996
Audit Committees	Jul 1997
Cash Management	Mar 1999
Commonwealth Agency Energy Management	Jun 1999
Controlling Performance and Outcomes	Dec 1997
Core Public Sector Corporate Governance, Principles for (includes Applying Principles and practice of Corporate Governance in Budget Funded agencies)	1997
Corporate Governance in Commonwealth Authorities and Companies–Principles and Better Practices	Jun 1999
Financial Statements Preparation	1996
Life-cycle costing in the Dept of Defence (in Audit Report No. 43 1997–98)	1998
Managing APS Staff Reductions	Jun 1996
Managing Parliamentary Workflow	Jun 1999
Management of Accounts Receivable	Dec 1997
Management of Corporate Sponsorship	Apr 1997
Management of Occupational Stress in Commonwealth Agencies	Dec 1998
New Directions in Internal Audit	Jul 1998
Paying Accounts	Nov 1996
Protective Security Principles (in Audit Report No.21 1997–98)	
Public Sector Travel	Dec 1997
Return to Work: Workers Compensation Case Management	Dec 1996
Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	Oct 1998
Telephone Call Centres	Dec 1996
Telephone Call Centres Handbook	Dec 1996