The Auditor-General
Audit Report No.22 2000–2001
Performance Audit

# Fraud Control in Defence

## Department of Defence

Australian National Audit Office

ISSN 1036-7632

ISBN 0 642 44256 8

Australian National
Audit Office

Canberra ACT
14 December 2000

Dear Madam President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in the Department of Defence 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 *Fraud Control in Defence.*

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 Manager
John Guilfoyle

# Contents

# Abbreviations

| | |
|---|---|
| ANAO | Australian National Audit Office |
| *CEIs* | *Chief Executive Instructions* |
| CLEB | Commonwealth Law Enforcement Board |
| CSP | Commercial Support Program |
| DFCP3 | Defence Fraud Control Plan No.3 |
| DFCP4 | Defence Fraud Control Plan No.4 |
| DRP | Defence Reform Program |
| *FMA Act* | *Financial Management and Accountability Act 1997* |
| MAB | Management Audit Branch |
| PSP | Professional Service Providers |
| SDSS | Standard Defence Supply System |

# Summary and Recommendations

# Summary

## Background

**1.** Fraud means obtaining money or other advantages by dishonest means. It is not restricted to monetary or material benefits and includes intangibles such as information. Fraud control in the public sector is the protection of public property, revenue, expenditure, rights and privileges from fraudulent exploitation.

**2.** The value of fraud committed in the Australian public sector is not known. A recent ANAO survey of fraud arrangements in Commonwealth agencies, including Defence, found that the level of fraud is difficult to measure. A reason for this is that different definitions of fraud are used across the Commonwealth. The Australian Institute of Criminology has estimated that, in the public and private sectors, '*fraud costs the community between $3 billion and $3.5 billion per year. This makes fraud the most expensive category of crime in Australia*.'

**3.** The Attorney-General's Department is responsible for administration of Commonwealth fraud control policy. The Chief Executive Officer of each Commonwealth agency is responsible for implementing a fraud control plan for the agency and for reporting to the Portfolio Minister on fraud control.

**4.** Defence expenditure amounts to $13 billion a year. Defence controls assets valued at some $41 billion. The magnitude of detected fraud affecting Defence in 1999–2000 was a comparatively low $2.5 million.

**5.** The objective of this audit was to establish whether Defence has developed sound fraud control arrangements that are consistent with better practice and fulfil its responsibilities for the protection of public property, revenue, expenditure, and rights and privileges from fraudulent exploitation. The audit was one of a series of audits of fraud control arrangements in Commonwealth agencies.

## Overall conclusion

**6.** The level of detected fraud in or against Defence is low. Nevertheless, fraud control in Defence could be improved, particularly in corporate governance and fraud intelligence, which underpin the fraud control process. Specifically, the Defence Audit Committee could give more attention to monitoring and developing Defence's fraud control plans.

**7.** Defence does not have a suitable fraud intelligence capacity. It should develop such a capacity to identify factors that may increase the risk of fraud and to enhance its fraud prevention and detection ability. A fraud intelligence capacity would also enable Defence to benchmark its fraud control work against comparable organisations and would enhance fraud risk assessment. A limited comparison with the UK suggests that fraud in or against Defence may be underestimated.

**8.** Defence could also address a number of issues concerning the fraud risk assessment process. These concern the delays between assessing risks and developing fraud control plans, the level of feedback to Groups[1] on fraud related matters and the qualifications of personnel engaged in the process.

**9.** The development of the Defence fraud control plan and Group and Project fraud control plans has not been timely. In addition, performance indicators included in most of the completed plans do not allow achievement of the objectives in the plans to be assessed.

**10.** Defence could also make improvements concerning a number of operational issues relating to fraud awareness and fraud investigations.

---

[1] Defence Groups are the administrative equivalent of Departmental Programs. The Group structure referred to in this report was amended on 1 July 2000.

# Key Findings

## Corporate governance (Chapter 2)

**11.** Fraud control arrangement in the context of Defence's corporate governance could be improved in three key areas. Firstly, Defence should comply with the Commonwealth fraud control policy requirement that agencies are to review their fraud control arrangements every two years. It would be appropriate to amend Defence's Chief Executive Instructions (CEI) to reflect this requirement.

**12.** Secondly, the Defence Audit Committee could usefully monitor Group and Sub-Group fraud control plans in accordance with the CEIs. With such monitoring, a higher priority might be assigned to the numerous fraud control plans in Defence.

**13.** Finally, more attention could be given to reporting in the Groups on compliance with fraud control plans. Some Groups may find it useful to include fraud control issues in their Group performance assessment arrangements.

## Fraud intelligence (Chapter 3)

**14.** Defence lacks a suitable fraud intelligence capacity. Analysis of important factors in the Defence environment would help in assessing the risk of fraudulent activity. Benchmarking Defence's fraud control work against that of comparable organisations would help in assessing whether Defence has under-estimated the extent of fraud in or against Defence.

**15.** A sound fraud intelligence capacity would allow for a more-informed approach to developing measures to enhance Defence's fraud prevention and detection ability.

## Fraud risk assessment (Chapter 4)

**16.** Improvements could be made in relation to the fraud risk assessment process adopted by Defence. The use of risk assessment plans that are up to four years old in the development of fraud control plans does not represent sound fraud control practice. All fraud control plans should be based on recent fraud risk assessments to ensure that the plans reflect the current circumstances.

**17.** Action to meet the request by Defence Groups for more feedback on fraud related matters would be beneficial in developing future Group and Sub-Group fraud risk assessments.

**18.** The current position in relation to the level of relevant competency qualifications held by personnel involved in the management of fraud, and the conduct of fraud risk assessments and planning activities, also requires attention.

## Fraud control plans (Chapter 5)

**19.** The ANAO reviewed Defence's three levels of fraud control plans and found that many areas within Defence have not developed the required plans. The Inspector-General Division considers that '*fraud control has not been accorded high priority by some Groups in Defence*'.[2] Defence must ensure timely development of all fraud control plans that are required to be developed under the existing Defence fraud control plan.

**20.** Most of the performance indicators included in the Defence fraud control plan and Group and Project fraud control plans are not measurable. Qualitative assessment in some aspects of fraud control is important, but a lack of measurable indicators inhibits a sound performance assessment process from operating within Defence in respect of fraud control.

## Defence ethics and fraud awareness (Chapter 6)

**21.** The ANAO examined various aspects of the operations of the Directorate of Fraud Control Policy and Ethics. In the ANAO's view, Defence should prepare for an increase in demand for ethics and fraud awareness sessions that is expected to result from development of fraud control plans at the Group and Sub-Groups level. This planning process has drawn many managers' attention to the need for such education and training.

**22.** A system of scheduling ethics and fraud awareness sessions is required in Directorate of Fraud Control Policy and Ethics to assist in forming medium and long term resourcing decisions.

**23.** Formal arrangements have not been developed to monitor staff attendance at ethics and fraud awareness sessions. In the absence of such arrangements, Defence is unable to assess compliance with the requirements of the various fraud control plans, at all levels, for staff to attend such sessions and take appropriate action.

---

[2] DAPEC Agendum No. 10/2000–17 May 2000: Proposed strategy for Defence Fraud Control Plan No. 4.

## Fraud investigations (Chapter 7)

**24.** Completion of a Defence-wide consolidated procedures manual for fraud investigations will be fundamental in providing a common approach to investigation of fraud in Defence.

**25**. Military police play a significant role in investigation of fraud in Defence. It is important that all relevant personnel obtain the appropriate competency qualifications.

## Response to proposed report

**26.** In response to the proposed report, Defence said that, overall, the report supports its efforts to implement effective fraud control across its many locations. It agreed to the ANAO's recommendations, except one relating to development of a suitable fraud intelligence capacity to support Defence's fraud risk assessment process, given its wide-ranging exposures.

# Recommendations

*Set out below are the ANAO's recommendations, together with report paragraph references and an indication of Defence's response. The ANAO considers that Defence should give priority to recommendations 1, 2 and 4.*

**Recommendation No.1 Para. 2.26**

*The ANAO recommends that Defence*:

a) amend its Chief Executive Instructions to comply with the Commonwealth fraud control policy requirement to review fraud control arrangements every two years;

b) ensure the Defence Audit Committee monitors Group and Sub-Group fraud control plans in accordance with Defence's Chief Executive Instructions; and

c) ensure that all Groups develop and comply with Group and Sub-Group fraud control reporting arrangements.

***Defence response:*** a) Agree.

b) Agree.

c) Agree.

**Recommendation No.2 Para. 3.34**

The ANAO recommends that Defence develop a suitable fraud intelligence capacity to support its fraud risk assessment process, given its wide-ranging exposures.

***Defence response:*** Disagree

**Recommendation No.3 Para. 4.20**

The ANAO recommends that Defence ensure that:

a) fraud control plans are based on recent fraud risk assessments;

b) the Groups receive appropriate advice on fraud-related matters to assist in fraud risk assessments; and

c) personnel primarily engaged in the management of fraud control as well as those primarily engaged in agency fraud risk assessment and planning activity obtain the proposed competency qualifications.

***Defence response:*** a) Agree.

b) Agree.

c) Agree.

**Recommendation No.4 Para. 5.17**

The ANAO recommends that Defence:

a) ensure timely completion of all Group, Unit and Project fraud control plans required by the Defence fraud control plan; and

b) include performance indicators in all Defence fraud control plans that allow regular assessment of progress.

***Defence response:*** a) Agree

b) Agree.

**Recommendation No.5 Para 6.14**

The ANAO recommends that Defence develop:

a) scheduling arrangements for the ethics and fraud awareness sessions to allow better medium and long-term resourcing decisions to be made in the Inspector-General Division; and

b) formal arrangements to monitor staff attendance at ethics and fraud awareness sessions.

***Defence response:*** a) Agree.

b) Agree.

**Recommendation No.6 Para. 7.14**

The ANAO recommends that Defence:

a) expedite the development of a consolidated and comprehensive set of fraud investigation procedures for Defence fraud investigations; and

b) ensure that military police undertaking fraud investigations have the competency standard required for personnel primarily engaged in the investigation of fraud.

***Defence response:*** a) Agree.

b) Agree.

# Audit Findings and Conclusions

# 1. Introduction

*This introduction outlines the fraud control arrangements within the Commonwealth public sector, provides background information on Defence and describes the audit objective, methodology and report structure.*

## Fraud control in the Commonwealth

**1.1** Fraud means obtaining money or other advantages by dishonest means. It is not restricted to monetary or material benefits and includes intangibles such as information. The Interim Ministerial Direction on Fraud Control defines fraud as:

> *…inducing a course of action by deceit or other dishonest conduct, involving acts or omissions or the making of false statements, orally or in writing with the object of obtaining money or benefits from or evading liability to the Commonwealth.*[3]

**1.2** The value of fraud committed in the Australian public sector is not known. The Australian Institute of Criminology has estimated that, in the public and private sectors, '*fraud costs the community between $3 billion and $3.5 billion per year. This makes fraud the most expensive category of crime in Australia*.'[4]

**1.3** Fraud control in the public sector is the protection of public property, revenue, expenditure, rights and privileges from fraudulent exploitation.[5] The fraud control policy of the Commonwealth Government states that:

> *The Commonwealth Government is committed to protecting its revenue, expenditure and property from any attempt, either by members of the public, contractors, sub-contractors, agencies, intermediaries or its own employees to gain by deceit financial or other benefits. This policy is designed to protect public money and property, protect the integrity, security and reputation of our public institutions and maintain a high level of services to the community consistent with the good government of the Commonwealth.*[6]

---

3 The Interim Ministerial Direction on Fraud Control is included in the Commonwealth Law Enforcement Board Guide, *Best Practice for Fraud Control*, AGPS, Canberra, 1994.

4 Australian Institute of Criminology Fraud Prevention and Control conference material 'Message from the Minister' 24-25 August 2000.

5 Draft Fraud Control Policy of the Commonwealth, Commonwealth Law Enforcement Board, 21 June 1999.

6 Fraud Control Policy of the Commonwealth in *Best Practice for Fraud Control*, op. cit.

**1.4** The Attorney-General's Department is responsible for the administration of the Commonwealth fraud control policy, including the development of investigation standards and investigator competencies, the provision of advice and guidance to agencies on all fraud control matters and reporting to government on how risks identified by agencies are being addressed.[7] The Department also reviews the quality of agencies' fraud assessment methodologies and fraud control plans to ensure that they comply with Commonwealth fraud control policy. A consultative process is under way to develop a revised fraud control policy.

**1.5** The Chief Executive Officer of each Commonwealth agency is responsible for implementing a fraud control plan for the agency and reporting on fraud control to the relevant Minister.[8]

## Fraud in Defence

**1.6** The Defence mission is *'to prevent or defeat the use of armed force against our country or its interests.'*[9] Defence expenditure amounts to $13 billion a year. Defence controls assets valued at $41 billion[10]. Defence has some 51 000 full-time military personnel and 20 000 Reservists,[11] in addition to 15 700 civilian Defence employees.

**1.7** The Secretary of the Department of Defence and the Chief of the Defence Force are jointly responsible for overall management of Defence through the exercise of their single and joint responsibilities under legislation and Ministerial directives. At the time of the audit fieldwork Defence was organised into twelve Groups[12]:

- *Defence Headquarters*
- *Army*
- *Intelligence*
- *Defence Personnel Executive*
- *Science and Technology*
- *Defence Information Systems*
- *Navy*
- *Air Force*
- *Support Command*
- *Acquisition*
- *Defence Estate*
- *Defence Corporate Support.*

---

7 These functions were until recently the responsibility of the Commonwealth Law Enforcement Board. The Attorney-General's Department formerly provided secretarial support.

8 Section 45 of the *Financial Management and Accountability Act 1997.*

9 'Defence' comprises the Department of Defence and the Australian Defence Force, which in turn comprises the three Services: Navy, Army and Air Force.

10 The net value of Defence assets as at 30 June 2000 equals the gross value ($61.943 billion) minus accumulated depreciation ($21.262 billion).

11 This figure does not include the Inactive Reserve Component.

12 Defence Groups are the administrative equivalent of Departmental Programs. The Group structure referred to in this report was amended on 1 July 2000.

**1.8** The amount of detected fraud affecting Defence in 1999–2000 was $2.5 million. The determined losses due to fraud since 1 July 1994 are set out in Table 1.1. Indicative Inspector-General Division fraud investigation statistics for 1999–2000 are at Appendix 1. Issues relating to the fraud investigations database, from which these figures are drawn, are discussed in Chapter 7 and Appendix 1.

**Table 1.1**
**Determined losses due to fraud in Defence**

| Financial Year | Determined Losses ($ million) |
|---|---|
| 1994–1995 | 1.8 |
| 1995–1996 | 2.5 |
| 1996–1997 | 1.7 |
| 1997–1998 | 3.0 |
| 1998–1999 | 1.9 |
| 1999–2000 | 2.5 |

Source: Inspector-General Division

## Audit objective and methodology

**1.9** The Defence fraud control audit is one in a series of performance audits of fraud control arrangements in Commonwealth agencies. Defence was also included in a recent ANAO a survey of fraud arrangements in APS agencies.[13] The overall conclusion of the audit survey is at Appendix 2.

**1.10** The objective of this audit was to establish whether Defence has developed sound fraud control arrangements that are consistent with better practice and fulfil its responsibilities for the protection of public property, revenue, expenditure, and rights and privileges from fraudulent exploitation.

[13] Audit Report No.47 1999-2000 *Survey of Fraud Arrangements in APS Agencies*.

**1.11** The ANAO developed a set of fraud control audit criteria linked to the audit objective. These audit criteria, considered in the indicated Chapters of the audit report, were that Defence should have:

- appropriate corporate governance arrangements including sound fraud control monitoring and reporting systems (Chapter 2);
- a fraud intelligence capacity to support fraud risk assessment (Chapter 3);
- fraud risk assessments undertaken by appropriately trained personnel (Chapter 4);
- a fraud control plan endorsed by Attorney-General's Department and lower-level plans to address identified risks (Chapter 5);
- ethics and fraud awareness campaigns for all relevant staff (Chapter 6); and
- fraud cases investigated by appropriately qualified personnel (Chapter 7).

**1.12** The audit fieldwork was carried out between January and July 2000. It was undertaken primarily within the Inspector-General Division, which has operational responsibility for Defence fraud control policy and undertakes civilian and major military fraud investigations. The Division also conducts ethics and fraud awareness sessions for Defence personnel.

**1.13** Audit fieldwork extended to personnel with responsibility for fraud control in each Defence Group. The military police, including the Provost Marshals[14] from each of the three Services, were also involved in the audit.

**1.14** Information on particular aspects of the audit was provided by the Attorney-General's Department and the Public Service and Merit Protection Commission (PSMPC).

**1.15** The ANAO reported on Defence procedures for dealing with fraud in 1991.[15] Although legislation and policy on fraud have been revised since then, a number of issues raised in that report were relevant to this audit report. These are referred to in the relevant Chapters of the audit report.

---

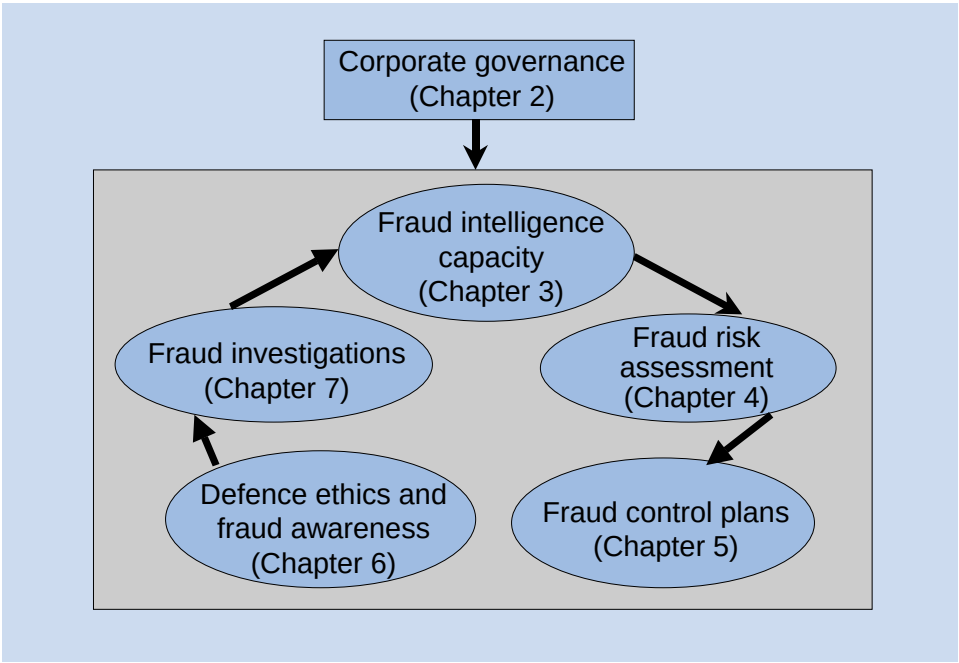
[14] The heads of each of the three Services' military police.

[15] Audit Report No.15 1991-92 *Department of Defence—Procedures for Dealing with Fraud on the Commonwealth*.

**1.16** The audit was conducted in conformance with ANAO auditing standards and cost $174 000.

**1.17** Figure 1.1 sets out the structure of this audit report.

**Figure 1.1**
**Structure of the audit report**



# 2. Corporate Governance

*This Chapter examines Defence fraud control activities in the context of its corporate governance structures. Recommendations are made concerning the Chief Executive Instructions and monitoring and reporting arrangements.*

**2.1** *'Corporate governance is the system by which an organisation is directed and controlled.'*[16] The fraud control policy of the Commonwealth is designed to manage fraud risks within a framework of sound corporate governance.

**2.2** The Secretary of the Department of Defence has indicated a close interest in Defence corporate governance. In an address at the National Press Club the Secretary noted that:

> *Defence is probably the biggest and most complex organisation in Australia—second only to Coles Myer as Australia's largest employer.*[17]

**2.3** He went on to say that there was widespread dissatisfaction with the general performance of Defence, there was poor performance accountability and a need to get corporate processes and systems right to enable and sustain a substantial improvement.

**2.4** The Secretary also recently pointed out that:

> *The size and complexity of Defence means that good governance—accountability for legislated requirements and performance to the Government's expectations—can never be taken for granted. Good governance steers an organisation through turbulent times, just the sort of times we have been facing in Defence. Good governance sets the direction and ensures that progress is being made towards long term goals.*[18]

**2.5** Good governance also helps create an environment inimical to fraud. The ANAO examined the Defence corporate governance arrangements as they affect fraud control. Attention was given to the reporting procedures that operate at various levels within Defence.

---

[16] Guidelines for managing risk in the Australian and New Zealand Public Sector, Standards Australia/ Standards New Zealand, HB 143: 1999.

[17] Dr Allan Hawke, Secretary, Department of Defence *What's the Matter – A Due Diligence Report* 17 February 2000, The National Press Club.

[18] Defence Media Release (26 June 2000).

## Responsibility/accountability framework

**2.6** The primary responsibility for fraud control rests with the Chief Executive of each Commonwealth agency. Section 45 of the *Financial Management and Accountability Act 1997* states that a Chief Executive must implement a fraud control plan for the agency and that fraud for that purpose includes fraud by persons outside the agency in relation to activities of the agency. The Finance Minister's Orders made under the Act require the Chief Executive to report on fraud control to the Minister responsible for the agency.

**2.7** The Act also requires each Chief Executive to establish and maintain an audit committee. The Defence Audit Committee's[19] terms of reference provide that it is responsible to the Secretary of the Department, as Chief Executive, for (among other things):

- establishing a Defence fraud control plan and oversight of its implementation; and
- oversight of the conduct of ethics awareness activities in Defence.

**2.8** Defence's Chief Executive Instructions (CEI) state that the audit committee '*is responsible for monitoring the implementation of all Defence fraud control plans*'.[20]

**2.9** The Inspector General has primary responsibility in Defence for developing fraud risk assessment methodology and the fraud control plan. The Inspector General also has responsibility for undertaking investigations, recoveries, reviews and evaluations, managing the Defence ethics and fraud awareness campaign and developing anti-fraud and ethics policies.

**2.10** The Directorate of Fraud Investigation and Recovery and the Directorate of Fraud Control Policy and Ethics (FCPE) are part of the General Investigation and Review Branch in the Inspector-General Division.

---

[19] Until 30 June 2000 the committee was known as the Defence Audit and Program Evaluation Committee.

[20] CEIs, Para 118 (issued September 1999).

**2.11** The Directorate of Fraud Investigation and Recovery investigates allegations of fraud, questions of probity or breaches of due process involving Defence appropriations and recovery of assets and property. It provides the point of contact with relevant external agencies and has a policy and quality assurance role across Defence. It undertakes all civilian and major military fraud investigations. Separately, military police in each of the three Services investigate fraud as part of their normal duties. Some 85 per cent of all fraud cases in Defence are investigated by military police.

**2.12** The objective of the FCPE, in partnership with Group and Sub-Group managers, is to establish a values-based ethical resource management culture and probity framework that optimises ethical use of Defence resources and minimises fraud, waste and abuse. In accordance with the fraud control policy of the Commonwealth, the section develops the Defence fraud control plan and related fraud risk strategies and policies. It also manages the Defence ethics and fraud awareness campaign, including high-level policy research and analysis.

**2.13** At the Group level *'the Defence Executive has affirmed that Group managers are responsible for the minimisation and ultimately the elimination of fraud within their Groups.'*[21] There is a Defence requirement for each of the twelve Groups to develop Program level fraud control plans at the Group and Sub-Group level.[22]

## Fraud planning cycle

**2.14** Compliance with the Interim Ministerial Direction on Fraud Control requires agencies to review their fraud control arrangements *'every two years as a minimum.'*[23] The Commonwealth Law Enforcement Board's *Best Practice for Fraud Control* states that:

> *… agencies are required to review their fraud control arrangements at a minimum every two years; more frequently if necessary. That review entails:*
>
> - *conducting another risk assessment; and*
> - *developing a further two year program for fraud control which will rectify residual shortcomings in the procedures.*[24]

---

21 CEIs, Para 111.

22 CEIs, Para 117 and Defence Fraud Control Plan No.3, Figure 1.

23 Interim Ministerial Direction on Fraud Control, op. cit., Para 2.

24 Best Practice for Fraud Control, op. cit., Para 24.

**2.15** Defence's CEIs state that the Defence fraud control plan *'is to be reviewed every four years, which, in essence, will entail another risk assessment*.'[25] This timing does not comply with the timing specified above. Defence is aware of this inconsistency and has indicated that it will amend its Instructions.

## Reporting against plans to the Defence Audit Committee

**2.16** As indicated above, the Defence Audit Committee is the key committee with responsibility for fraud control in Defence. The current Defence fraud control plan is the third such document.[26] There were no structured reporting mechanisms in relation to the first two Defence fraud control plans.

**2.17** Reporting against Defence Fraud Control Plan No.3 (DFCP3) to the Committee was required *'12 months after the plan is formally promulgated'*[27]. DFCP3 was authorised by the Secretary of the Department and the Chief of the Defence Force in June 1998. In May 2000 the Inspector-General Division developed management progress reporting arrangements for the Groups, including a uniform reporting format, and obtained Group fraud control compliance information.

**2.18** The first report against DFCP3, based on these management progress reports, was provided to the Committee in September 2000. This means that reporting on compliance with DFCP3 was behind the schedule set out in DFCP3 by over a year. The ANAO was informed that the main reason for this delay was that a number of Groups were late developing approved Group fraud control plans. For instance, in September 1999 the Committee formally directed that all Groups have fraud control plans endorsed by the Inspector General by 31 December 1999[28] but, by January 2000, seven of the twelve Groups still did not have approved Group fraud control plans. This matter is discussed in Chapter 5.

**2.19** As mentioned above, the Committee is responsible for monitoring the implementation of all Defence fraud control plans. At the time of the audit fieldwork, the Committee had not monitored the implementation of Defence's Sub-Group or lower-level fraud control plans.

---

[25] CEIs, Para 119.

[26] Fraud control plans are discussed in Chapter 5 of this audit report.

[27] Defence Fraud Control Plan No.3, para 6.8.1.

[28] DAC minutes of 17 September 1999

## Reporting in the Groups

**2.20** At the Group level, there has been only limited reporting against Group and Sub-Group fraud control plans. This is partly because, at the time of audit fieldwork, two of the twelve Groups still did not have approved Group fraud control plans and, of the 89 Sub-Groups in Defence, only 47 had approved Sub-Group fraud control plans. Fraud control plans are discussed in Chapter 5.

**2.21** On a positive note, in a number of Groups where plans had been developed, the existing business performance assessment framework is also being used for fraud control monitoring and reporting purposes. This approach could be adopted generally in Defence for efficiency reasons and to assist in ensuring that fraud control is given appropriate priority.

**2.22** An examination of Group and Sub-Group fraud control plans revealed that many of the performance indicators in the plans are not measurable. The performance indicators require amendment as part of the further development of reporting arrangements within the Groups. Performance indicators are discussed in Chapter 5.

## Conclusion

**2.23** Defence should improve its corporate governance of fraud control arrangements in three key areas. Firstly, Defence is at present not complying with the Commonwealth fraud control policy requirement that agencies are to review their fraud control arrangements at a minimum of every two years. The Defence CEIs should be amended to reflect this requirement and measures developed to ensure compliance.

**2.24** Secondly, the Defence Audit Committee has not been monitoring implementation of Group and Sub-Group fraud control plans in accordance with the CEIs. If such monitoring occurred, a higher priority might be assigned to fraud control plans at these levels across Defence.

**2.25** Finally, there is only limited reporting on compliance with fraud control plans at the Group level and below. Some Groups may find it effective and efficient to include fraud control issues in their existing Group performance assessment arrangements.

## Recommendation No.1

**2.26** The ANAO *recommends* that Defence:

a) amend its Chief Executive Instructions to comply with the Commonwealth fraud control policy requirement to review fraud control arrangements every two years;

b) ensure the Defence Audit Committee monitors implementation of Group and Sub-Group fraud control plans in accordance with the Chief Executive Instructions; and

c) ensure that all Groups develop and comply with Group and Sub-Group fraud control reporting arrangements.

### *Defence response*

**2.27**

a) Agree, noting, however, that the difficulty of implementing cross-agency risk assessment in large and dispersed agencies such as Defence was recognised by the (then) Commonwealth Law Enforcement Board (CLEB). During consultation over the past three years aimed at revising the Fraud Control Policy of the Commonwealth, CLEB indicated that a fraud risk and planning cycle of between two to four years would be permitted depending on an agency's risk profile. This flexibility was also foreshadowed by CLEB on Page 2 of the Australian Federal Police's *ComFraud Bulletin No.5* of April 1997.

b) Agree. It was considered by the Defence Audit Committee in October 2000, and will be kept under review.

c) Agree.

# 3. Fraud Intelligence

*This Chapter examines fraud intelligence in Defence. It considers the environment in which Defence operates and provides some comparisons with UK Defence. A recommendation is made on developing a fraud intelligence capacity.*

**3.1** An essential part of developing any organisation's risk management framework is establishing the strategic context in which the organisation operates. There is a need to '*define the relationship between the organisation and its environment, identifying the organisation's strengths, weaknesses, opportunities and threats*'.[29]

**3.2** The Directorate of Fraud Investigation and Recovery in the Inspector-General Division responds to cases drawn to its attention by, for instance, the Management Audit Branch[30], Defence staff or the public. The section does not undertake pro-active fraud prevention. In fact, the Inspector-General Division does not have any fraud intelligence capacity. With a fraud intelligence capacity, Defence could consider several key issues that might indicate areas of increased risk of fraudulent activity. It could analyse fraud control in comparable organisations and examine the environment in which Defence operates, with the aim of developing measures to eliminate fraud. A number of these issues are discussed below.

## Environmental issues

**3.3** A number of factors concerning the Defence environment need to be considered as part of any fraud intelligence capacity. Defence has undergone a series of significant changes in recent times. It is still, in essence, an organisation in significant transition. The major changes have resulted from efficiency and other reform programs. There have been significant changes by way of structural re-organisation, increases in outsourcing to contractors and reductions in the number of Defence personnel with some likely attendant loss of confidence, knowledge and memory. Financial management issues are also part of the environment relevant to fraud intelligence. Significant and/or systemic problems with administrative systems, and associated computerised systems, are important environmental factors that may increase the risk of fraudulent activities. A number of significant environmental issues are summarised below.

---

[29] Australian New Zealand Joint Standard on Risk Management, AS/NZS 4360: 1999, Para 4.1.3.

[30] Defence's internal audit branch.

## Efficiency and other reform programs

**3.4** Recent efficiency and other reform programs in Defence have resulted in an environment of significant change. Major programs of this nature have been the Commercial Support Program (CSP) and the Defence Reform Program (DRP). Introduced in 1991,[31] the CSP is a program for competitive tendering of support (non-combat) activities conducted 'in house' by civilians or Service personnel. It has resulted in a significant increase in Defence's use of contractors and consultants.[32] The DRP was introduced to implement recommendations that arose from the Defence Efficiency Review (1997), which examined Defence management with the aim of eliminating unnecessary administrative practices and duplication and to ensure the organisation was focussed on core functions.

## Staff reductions

**3.5** In the early 1990s Defence had approximately 70 000 full-time military personnel and 25 000 civilian staff.[33] Largely as a result of the efficiency and other reform programs, these numbers have been reduced to 51 000 full-time military personnel and 15 700 civilian employees respectively. There has been an increase in private sector assistance in Defence from contractors, consultants and professional service providers, but, as noted earlier, some likely loss in corporate memory.

## Military ethos

**3.6** Military service is different from civilian employment in Defence and most other areas of the Australian Public Service. A survey conducted as part of a recent ANAO audit on retention of military personnel found that the appeal of the military ethos and way of life were prime motivators for people to enlist in the Services. An overwhelming proportion of new recruits indicated that they joined the Services for a career.[34] A culture of loyalty (for example, to a commander, unit or Service) and an attitude of 'getting the job done' are instilled in recruits. These characteristics of military culture are positive but there is potential for ambiguity to arise if there is an apparent conflict of loyalties. The Inspector-General Division has developed fraud awareness videos as part of an attempt to address topics such as the ethical issues that can arise out of a conflict of loyalties.[35] These videos are screened during ethics and fraud awareness sessions. Ethics and fraud awareness are discussed in Chapter 6.

---

[31] The Commercial Support Program followed *The Defence Force and the Community* (the Wrigley Report), tabled by the Minister for Defence in 1990.

[32] The Inspector-General Division in 1999 completed only one fraud investigation involving a contractor.

[33] Defence Review 2000 – Our Future Defence Force, A Public Discussion Paper, June 2000, p52.

[34] Audit Report No.35 1999-2000 *Australian Defence Force—Retention of Military Personnel*.

[35] Defence fraud awareness videos of this nature include 'The Brutus Award' and 'Unwritten Contract'.

## Financial and administrative systems

**3.7** Defence is aware that its financial management is an area in need of enhancement. The ANAO raised several matters that point to the need for significant improvement in systems integrity and governance, during the audit of Defence's financial statements for 1998–1999. These matters included:

- the Department found assets not previously recorded to the value of $1.4 billion;
- the Standard Defence Supply System (SDSS) has major problems with general functionality and inventory quantities, prices, and classifications:
  - the SDSS system recorded 3863 fixed asset groups at fifty cents per item. The ANAO estimates the understatement at $350 million;
  - the SDSS system does not record all rotable/repairable items. The size of the understatement is unquantifiable; and
  - key asset management data is not collected. The costs of maintaining assets are an important element of informed replace/retain decisions.[36]

**3.8** The audit of the financial statements for 1999–2000 raised similar issues. It said that business process failure and stocktake deficiencies indicated by significant quantity variances in repairable items recorded on the Standard Defence Supply System increased the scope for employee fraud.[37]

**3.9** Several ANAO performance audit reports have commented adversely on aspects of Defence financial management and administration, particularly in relation to Defence acquisition and facilities projects. Defence's Management Audit Branch reports have also made adverse comment on Defence systems. For example, a MAB report on cost recovery and debtor management highlighted significant problems in debt recognition, recording and management in Defence.[38]

---

[36] Source: ANAO: Department of Defence, 1998-99 Financial Statements Audit Report, October 1999.

[37] DAC – Secretarial Note No.26/2000, September 2000.

[38] Management Audit Branch: Audit of Accounts Receivable for 1999/2000 (2000/11760, June 2000).

**3.10** The Minister for Defence recently stated that there are:

> *… significant areas which defence must challenge and meet in the year 2001. First and foremost is financial management. Over the years, probably over decades, financial management is something which has completely passed defence by. Its reputation in government for defence financial management is very poor. The challenge to defence figures is consistent, and the challenge of getting defence matters up against unreliable figures is an immensely difficult task for whoever the Minister of the day might be.*[39]

**3.11** The Secretary of the Department has commented on difficulties associated with a number of Defence transaction processing systems as follows:

> *You might like to reflect on the fact that Defence now has:*
>
> ***PMKEYS*** *– a People Soft personnel application;*
>
> ***ROMAN*** *– a SAP solution to facilitate financial management; and*
>
> ***SDSS*** *– a Mincom product to support our materiel function.*
>
> *Each of these is, remarkably, based on a different chart of accounts! They can't, don't or won't talk to each other, other than under extreme duress through extraordinarily complicated interfaces and 'hydraulics' at the end of the financial year. They even give us different answers to the same question – for example, the cost of personnel…*
>
> *In other words, they are transaction processing systems that do not readily produce meaningful management information. The absence of a simple data dictionary compounds the problem of communication between these corporate systems – each describes the same data differently and the apples with oranges comparison is the inevitable outcome.*[40]

---

[39] The Hon. John Moore, MP—Minister for Defence: address to Royal United Services Institute of Australia, Triennial International Seminar, Canberra, 16 November, 2000.

[40] An address by the Secretary of the Department of Defence, Dr Allan Hawke, on 25 August 2000.

## Defence procurement and project management

**3.12** The UK National Audit Office reported in 1995 on the risk of fraud in procurement in the Ministry of Defence.[41] An audit review was initially requested by the Chief of Defence Procurement. The need for such a review was subsequently reinforced by the convictions in 1993 and 1994 of three former Ministry of Defence officials. One case was estimated to have involved at least £3 million in corrupt payments, including significant sums from overseas contractors.

**3.13** The NAO said that it was difficult to quantify the amounts lost as a result of fraud in Defence. For 1993–94 the estimated value of possible frauds under investigation by Ministry of Defence Police was about £22 million, but not all of this was possible procurement fraud. The NAO noted that this was low in an organisation that let about 50 000 contracts a year and that had a procurement budget exceeding £9 billion and a total Defence budget of £23 billion.

**3.14** The NAO report commented that the scope for fraud in large procurement projects was limited by the extent of checks and the involvement of others. There are so many players and controls in such projects that major frauds are difficult to achieve if prescribed controls are operated as intended and staff are vigilant and well motivated. The three fraud cases that have come to court did not involve large procurement projects.

**3.15** Of greater concern to the NAO were areas where control systems were likely to be less comprehensive or where changes in management arrangements had altered the circumstances in which controls operated. Risk areas were computer systems, non-competitive pricing, small value non-competitive contracts, local purchase arrangements, and control of assets held by contractors. The NAO was generally satisfied with the Ministry's action and proposed action regarding procurement fraud. These included establishment of a Defence Fraud Unit to coordinate fraud training and act as a focus for fraud minimisation in the Ministry. The report set out useful advice on fraud control measures in procurement.

**3.16** The NAO report also prompted the Ministry to consider private sector practices such as corporate fraud risk analysis, particularly at the interface between systems for accounting, bill-paying and other computerised systems. The NAO also noted that a number of companies,

---

[41] National Audit Office (UK) *Ministry of Defence: The Risk of Fraud in Defence Procurement* (1995).

by means of employment contracts, ban employees from working for suppliers up to three years after leaving their employment.[42]

**3.17** In Australia, Defence spends more than $2 billion a year on progressing more than 200 major capital equipment acquisition projects with a total approved cost in excess of $40 billion. Several ANAO reports on this area of Defence activity have raised issues concerning Defence management of acquisition projects and contracts.[43]

**3.18** **Particular issues concerned payments made ahead of work** performed; payments made for unsatisfactory work; senior management pressure on project staff to spend the Defence budget before annual appropriations lapsed; inadequate records of payments; project management and contract administration by staff inexperienced and untrained in such matters; and insufficient higher-level oversight of major project progress. Although ANAO reports are distributed to Defence Audit Committee members the committee has not formally reviewed any of them. Issues raised in those reports are relevant to any assessment of fraud risks.[44]

**3.19** In discussion with the ANAO on its proposal that Defence have a fraud intelligence capacity, the Inspector General indicated that detected fraud in Defence was too small to justify such a capacity and that Defence would be better served by improving its management of acquisition projects and contracts. Although the ANAO considers that a fraud intelligence capacity should be developed[45] it does agree with the Inspector General that improvements in project management and business practices would help to avoid opportunities for fraud. A recent General Accounting Office report on program risks in US Defense urged action on financial control weaknesses that created an environment that made Defense vulnerable to fraud (refer Appendix 3).

---

[42] Defence in Australia does not have a ban of that kind. The Public Service and Merit Protection Commission in Australia may include in the *Guidelines on Official Conduct of Commonwealth Public Servants* a suggestion that, when outsourcing, agencies consider including a provision in contractual arrangements restricting for a specified period the subsequent employment by the successful tenderer of key-decision makers in the outsourcing tender process.

[43] For example, Audit Report No.34 1997-98 *Department of Defence—New Submarine Project* and Audit Report No.13 1999-2000 *Department of Defence—Management of Major Equipment Acquisition Projects*.

[44] Defence indicated that there had been developments since the ANAO audit began in February 2000. Defence said that it has been policy since February 2000 to provide all audit reports, with a note indicating whether there were potential matters of concern, to each member and observer on the Committee. Defence also said that the Committee follows up implementation of audit recommendations and has now made specific provision at each meeting for members and observers to provide comments. Since February 2000 the Committee has considered three papers on Defence fraud control planning and has progressed departmental action on implementation.

[45] Refer Fraud Intelligence Capacity section below.

**3.20** Improvement in Defence's project management is proving to be a long-term endeavour. It does not diminish the need for an intelligence capacity that would help in detecting fraud and devising measures to counter it. Risks of unsatisfactory or irregular practices are likely to increase with Defence's increasing use of contractors to administer contracts. The Defence Acquisition Organisation employs Professional Service Providers (PSPs) to assist in contract management. The number of PSPs on-site in DAO had increased from 215 in December 1997 to 356 in April 1999. Other PSP contracts involved DAO work off-site in contractors' premises.[46]

## Defence property management

**3.21** The UK National Audit Office recently reported on fraud risk in Ministry of Defence property management.[47] The report stated that property management cases represented some 50 per cent by number and 75 per cent by value of all frauds then being investigated by the Ministry. The Ministry recognised that property management was an area susceptible to fraud but the report concluded that the Ministry's current level of control against fraud was unacceptably low. The NAO recommended that the Ministry:

- reappraise its whole property management control environment in the light of increased contractorisation and changed business practices;
- ensure that it collects basic data relevant to fraud risk management; and
- review the balance of resourcing between units analysing, detecting and helping to prevent fraud, and those investigating suspected fraud, because resourcing appeared heavily biased towards investigation over detection and prevention.

**3.22** The Ministry spends some £900 million a year on property management. The total estimated fraud loss of those cases under investigation by the Ministry's Police Fraud Squad was £17 million.

**3.23** The UK fraud loss estimates in the Australian context would be equivalent to $15.2 million in cases under investigation in the Defence Estate Organisation alone.[48] As stated in Chapter 1, the magnitude of

---

[46] Audit Report No13 1999–2000 p. 138.

[47] National Audit Office (United Kingdom) *Ministry of Defence—The Risk of Fraud in Property Management* (18 May 2000).

[48] Based on 1998–99 expenditure of $803.8 million on approximately equivalent functions in Defence (ie. resources and policy, property management and estate operations and planning).

detected fraud affecting the whole of the Defence organisation in 1999–2000 was $2.5 million and annual determined losses in Defence since 1994–95 have not exceeded $3 million. On the face of it, the comparison with the UK indicates that detected fraud may not represent the extent of actual fraud in Defence.

**3.24** The ANAO's first performance audit in the area of Defence property concerned delivery of facilities projects by Defence Estate Organisation (DEO).[49] The report, tabled in April 2000, commented favourably on DEO's project delivery and business practice innovations in meeting Defence clients' needs but stated that financial management should be improved. The audit disclosed significant breakdowns in internal controls over payment of Commonwealth funds. On one major construction project, $37 million was paid to contractors as prepayments for materials that were neither listed in invoices nor verified before payment. This was part of a strategy to expend funds before relevant appropriations lapsed.

**3.25** The audit report commented that these transactions reflected poor practice and were contrary to the CEIs and inconsistent with proper management of Commonwealth funds. The audit report was not reviewed by Defence's audit committee.

**3.26** At the time of audit, DEO's financial information was drawn from three sources: DEFMIS, ROMAN and PMKEYS (which contains payroll and personnel information). DEO considers that the difficulties caused by the use of three separate systems are compounded by Defence's ongoing project to modify the systems so that they report on an accrual accounting rather than cash basis. As a result, DEO has had considerable difficulty in validating their financial data. An internal DEO document stated that DEO's financial data is never absolutely accurate, and that it is not uncommon for DEFMIS and ROMAN to vary by several million dollars, with no way of judging which system is more accurate.[50] This has had an impact on DEO's ability to manage accurately its expenditure against pre-determined budget targets.

**3.27** Management Audit Branch is considering a national audit on contracting outside the Defence Acquisition Organisation and units as it has identified that '*overall, Defence has a low level of experience in the area of contract management*'.[51]

---

[49] Audit Report No.37 1999–2000 *Department of Defence—Defence Estate Project Delivery.*

[50] Director Facilities Resources and Programming Section Minute to HDE 'DEO Budget Management (DFRP 29/2000)', 5 April 2000.

[51] DAC Agendum 7/2000, 28 March 2000, Management Audit Branch, Medium Term Audit Strategy 2000/2003.

## Fraud intelligence capacity

**3.28** The ANAO's 1991 report on procedures for dealing with fraud in Defence recommended that '*Defence continue to develop, and encourage the use of, analytical techniques and audit tests designed to detect the existence of, or potential for, fraudulent transactions.*'[52] Defence accepted the recommendation. The 2000 audit found that Defence has not developed or used the recommended techniques and tests. Defence does not have a fraud intelligence capacity.

**3.29** Defence should undertake regular extensive benchmarking to compare its operations with those of other organisations spending considerable amounts of public funds. These would include other nations' defence departments.

**3.30** As recommended by the NAO for the UK Ministry of Defence, a fraud intelligence capacity would assist in understanding fraud risks. Information on potential fraud risks could be derived by, for example, examining the patterns and relationships of existing Defence information. Extraction of fraud investigation data from the new linked investigation database (discussed in Chapter 7), coupled with sound analytical techniques, should assist Defence in assessing its fraud risks and adopting measures to enhance its fraud prevention and detection ability.

**3.31** The ANAO is aware of Defence's reluctance to develop a fraud intelligence capacity arises from a concern to avoid unnecessary costs as detected fraud affecting Defence has only averaged about $2.2 million per annum over the last six years.[53] Such a capacity should, however, focus on the fraud that is estimated could occur, (particularly in a changing environment that is likely to include risks greater than, and different from, those experienced in the past) and not just on those frauds that are detected. Development and maintenance of a credible capacity need not be resource-intensive.

## Conclusion

**3.32** Defence does not have a suitable fraud intelligence capacity. There is no analysis of important factors in the Defence environment that may increase the risk of fraudulent activity. Nor does Defence benchmark its fraud control work against comparable organisations. These issues warrant further consideration. For instance, admittedly a limited international comparison suggests that fraud in Defence may be underestimated.

---

[52] Audit Report No.15 1991–92 *Department of Defence—Procedures for Dealing with Fraud on the Commonwealth*, Recommendation No.26.

[53] Refer Table 1.1.

**3.33** A sound fraud intelligence capacity would support the assessment of fraud risk. Fraud risk assessment is discussed in detail in Chapter 4. It would also allow for a more-informed approach to developing measures to enhance Defence's fraud prevention and detection ability.

## Recommendation No.2

**3.34** The ANAO *recommends* that Defence develop a suitable fraud intelligence capacity to support its fraud risk assessment process, given its wide-ranging exposures.

### *Defence response*

**3.35** Disagree, fraud in Defence is predominantly opportunistic, of comparatively small amounts, and good coverage is already provided by, for example, Service police, regional security and audit personnel. The cost of establishing an intelligence capacity would thus not seem to represent good value-for-money.

### *Audit comment*

**3.36** A fraud intelligence capacity should focus on estimated possible fraud as distinct from detected fraud. Currently there is no analysis of significant environmental factors in Defence that could influence fraudulent activities, nor does Defence benchmark fraud activities and exposures in Defence against those in comparable organisations. A fraud intelligence capacity need not be resource-intensive. It would, however, significantly support fraud risk assessment and enhance fraud prevention and detection. In turn, this would provide greater assurance at reasonable cost to all stakeholders. This analysis is essentially one for Defence management to undertake and satisfy itself that its fraud prevention/detection strategies and initiatives are sufficient for the task, given its wide-ranging exposures.

# 4. Fraud Risk Assessment

*This Chapter examines some of the issues associated with fraud risk assessment in Defence and makes recommendations concerning the timeliness and consistency of risk assessments, as well as feedback and training arrangements.*

**4.1** Commonwealth fraud control policy states that *'a risk assessment methodology must be capable of 'green fields' measurement of the risk of fraud.'*[54] In June 1999 the Commonwealth Law Enforcement Board (CLEB) released, as a consultation draft, a proposed new fraud control policy of the Commonwealth. The proposed Fraud Control Guideline No.1 gives agencies two options from which to choose in adopting a fraud risk assessment methodology.[55] These options are the 'green fields' measurement of the risk or the use of the Australian New Zealand Joint Standard on Risk Management.[56]

**4.2** Defence Fraud Control Plan No.3 (DFCP3) is based on a fraud risk assessment undertaken in 1996. Defence engaged the Australian Bureau of Statistics to provide statistical advice and assistance with the design of the assessment process to meet the requirements of the fraud control policy of the Commonwealth. The assessments were subject to a validation exercise that was completed in May 1997. The validation covered eight per cent of the survey responses from selected eastern state units and included every Group and the range of functions identified by the initial risk assessments as having a very high or high residual risk. The team assessed the:

- extent of local management initiatives;
- quality and value of these initiatives;
- effect of the initiatives in possible cases of prosecution; and
- risk assessment position.[57]

---

54 Interim Ministerial Direction on Fraud Control, op. cit.

55 Draft Fraud Control Policy of the Commonwealth, op. cit., Fraud Control Guideline No.1.

56 AS/NZS 4360: 1999.

57 Defence Fraud Control Plan No.3, para 5.6.2.

**4.3** Defence has indicated the future direction of its risk assessment methodology in its document *Defence strategy for Defence Fraud Control Plan No.4* (DFCP4). The Defence Audit Committee has agreed to adopt the Australian New Zealand Joint Standard on Risk Management in the development of the fraud risk assessment associated with the proposed DFCP4. This is consistent with the proposed Fraud Control Guideline No.1.

**4.4** The key components of this methodology are:

- an assessment of risk (in relation to the organisation's underlying operations) to ensure appropriate attention is directed to areas of greatest exposure/vulnerability;
- consideration of controls to address the risks of fraud;
- an assessment of any residual risk; and
- the development of a program for the ongoing control of risk in the future.

**4.5** The ANAO examined some key issues associated with the fraud risk assessment process adopted by Defence.

## Timeliness

**4.6** All but one of the twelve Groups have fraud control plans approved by the Inspector General. The Inspector General has approved ten of these plans[58] since September 1999.[59] At the Sub-Group level only 47 of the 89 required fraud control plans have been developed.[60] Most of the fraud control plans that have been developed by the Groups and Sub-Groups have been based on the 1996 fraud risk assessment.

**4.7** As outlined in Chapter 3, Defence has undergone major change in recent years. In the period since the fraud risk assessment, the Defence Reform Program, introduced in 1997 after the Defence Efficiency Review, has changed Defence's organisational structures. These changes affect the current validity of the 1996 assessment.

---

[58] Refer Table 5.1.

[59] In September 1999 Defence's audit committee formally directed that all Groups have fraud control plans endorsed by the Inspector General by 31 December 1999 (DAPEC minutes of 17 September 1999).

[60] Refer Table 5.2.

**4.8** A number of Groups conducted new risk assessments before developing their latest fraud control plans. This was mainly because the Groups considered that the original assessment no longer reflected their fraud risks or that the area concerned was established after the 1996 risk assessments. In some cases consultants were engaged to undertake the new assessments.

**4.9** It is important that all fraud control plans are based on recent fraud risk assessments to ensure that the plans reflect evaluations of the existing fraud risks confronting the entities subject to the plans. Management involvement at all levels is essential if the risks are to be identified, assessed, treated and monitored in a manner that provides suitable assurance and confidence to all internal and external stakeholders.

## Feedback

**4.10** Feedback on recent fraud cases and associated issues is an important source of information to Groups attempting to assess the fraud risk confronting their operations.

**4.11** On closure of a fraud case, the Group or Groups involved in the case are provided with a report on the investigation. In addition, the Inspector-General Division publishes a newsletter that contains fraud case studies. It has also developed a website accessible by 85 per cent of Defence personnel.

**4.12** Group Coordinators[61] informed the ANAO that they were aware of these resources. They considered, however, that provision of more Defence-wide fraud control information would better inform fraud control decision-making. The type of information they envisage would include feedback on the number and type of fraud cases undertaken across Defence. Feedback on fraud cases has been hampered by the difficulties in obtaining uniform Defence-wide statistical information on fraud (discussed in Chapter 7).

## Training

**4.13** The proposed Fraud Control Guideline No.1 states that *'agencies should move as quickly as practicable … to ensure that all personnel who are primarily engaged in the prevention, detection and investigation of fraud meet the required fraud control competency standards as established on the Australian National Training Register.'*[62]

---

[61] A Group Coordinator has operational responsibility for fraud control in the Group.

[62] Draft Fraud Control Policy of the Commonwealth, Fraud Control Guideline No.1, op. cit.

**4.14** The proposed guideline also states that '*the Advanced Diploma, Fraud Control (Management) is the competency standard required for personnel primarily engaged in the management of fraud prevention, detection and investigation activity*' and that '*the Certificate IV, Fraud Control (Prevention/ Detention) is the competency standard required for personnel primarily engaged in agency fraud risk assessment and planning activity*'. Competency standards of this kind are not compulsory under the current fraud control policy of the Commonwealth.

**4.15** The ANAO found that no Defence personnel had formal competencies of this kind, although some may be capable of undertaking the duties. For instance, the Defence fraud risk assessment officer, employed within FCPE, has attended many conferences and seminars on risk assessment and risk management and has tertiary qualifications in mathematics. Defence has stated that the reason that no personnel had achieved these competencies was that, until recently, training of this nature had not been available in Canberra.

**4.16** To comply with the proposed Fraud Control Guideline No.1, Defence personnel who undertake fraud risk assessment and planning activity (at least at the Group level) or are responsible for Defence-wide management of fraud prevention, detection and investigation activity will need to obtain formal competency qualifications. Defence informed the ANAO that it was intending to proceed towards obtaining such qualifications for relevant personnel.

## Conclusion

**4.17** Improvements could be made in relation to the fraud risk assessment process adopted by Defence. Firstly, the use of risk assessment plans that are up to four years old in the development of fraud control plans does not represent sound fraud control practice. All fraud control plans should be based on recent fraud risk assessments to ensure that the plans reflect the current circumstances.

**4.18** Action to meet the request by the Groups for more advice on fraud-related matters would be beneficial in developing future Group and Sub-Group fraud risk assessments.

**4.19** The current position in relation to the level of relevant competency qualifications held by personnel involved in the management of fraud, and the conduct of fraud risk assessments and planning activities, also requires attention.

## Recommendation No.3

**4.20** The ANAO *recommends* that Defence ensure that:

a) fraud control plans are based on recent fraud risk assessments;

b) the Groups receive appropriate advice on fraud-related matters to assist in fraud risk assessments; and

c) personnel primarily engaged in the management of fraud control as well as those primarily engaged in agency fraud risk assessment and planning activity obtain the proposed competency qualifications.

*Defence response*

**4.21**

a) Agree.

b) Agree.

c) Agree. Personnel primarily engaged in the management of fraud control will seek risk assessment qualifications. The extent to which those engaged in Group fraud risk assessment and planning activity obtain competencies, however, will be subject to resource availability and perceived benefits by Group managers and Commanders.

# 5. Fraud Control Plans

*This Chapter reviews Defence's three levels of fraud control plans. Recommendations are made for timely development of Group and Unit or Project fraud control plans and measurable performance indicators.*

**5.1** Defence has three levels of fraud control plans,[63] as indicated in Figure 5.1.

**Figure 5.1**
**Levels of Defence fraud control plans**

| ***Defence fraud control plan*** |
|---|
| This is the paramount Defence fraud control plan considered by the Audit Committee and endorsed by the Commonwealth Law Enforcement Board (CLEB). It is the plan that the Chief Executive is required to implement under section 45 of the *Financial Management and Accountability Act 1997* and under the fraud control policy of the Commonwealth. |
| ***Group fraud control plans*** |
| These plans are intended to meet the needs of the Groups. These are developed by the individual Groups and endorsed by the Inspector-General. These plans are a requirement of DFCP3. |
| ***Unit or Project fraud control plans*** |
| These plans are subordinate to the Program fraud control plans and are the responsibility of unit commanders or project managers. This level of planning is also required under DFCP3. |

Source: DFCP3

## Defence fraud control plan

**5.2** Since 1989 there have been three Defence fraud control plans. These plans have covered the following periods:

- Defence Fraud Control Plan No.1 – November 1989 to November 1991;
- Defence Fraud Control Plan No.2 – March 1993 to March 1995; and
- Defence Fraud Control Plan No.3 – July 1998 until replaced by DFCP4.[64]

**5.3** Defence Fraud Control Plan No.4 is being prepared for introduction in 2001.

---

[63] This requirement is set out in the Defence Fraud Control Plan No.3, Figure 1.

[64] As discussed in Chapter 2, compliance with the Interim Ministerial Direction on Fraud Control requires agencies to review their fraud control arrangements *'every two years as a minimum.'*

**5.4** As indicated above, there were long periods after the first and second plans when Defence had no fraud control plan. Defence said that, in those periods, it considered the previous plan was still in operation.

**5.5** CLEB approved Defence Fraud Control Plans Nos.1, 2 and 3 as meeting the requirements of the fraud control policy of the Commonwealth set out in the Best Practice for Fraud Control guide that incorporates the Interim Ministerial Direction on Fraud Control.

## Group fraud control plans

**5.6** The Inspector-General Division considers that '*fraud control has not been accorded high priority by some Groups in Defence*'.[65] The requirement for Groups to prepare fraud control plans was established with the approval of the DFCP3 in July 1998. As only one Group had developed such a plan in the year since the establishment of DFCP3, the Defence Audit Committee formally directed that all Groups have fraud control plans endorsed by the Inspector General by 31 December 1999.[66] This was not achieved by seven of the twelve Groups. In an attempt to encourage compliance, Groups were advised by the Inspector-General Division that the ANAO was undertaking this audit of fraud control arrangements.

**5.7** Table 5.1 provides approval details for the Group fraud control plans. It shows that development of Group fraud control plans has not been timely.

---

[65] DAPEC Agendum No. 10/2000—17 May 2000: Proposed strategy for Defence Fraud Control Plan No. 4.

[66] Defence Audit Committee requirement (DAC minutes of 17 September 1999).

**Table 5.1**
**Group fraud control plans**

| *Group*[1] | *Fraud Control Plan?* | *Date Approved by Group Head* | *Date Approved By Inspector General* |
|---|---|---|---|
| Defence Headquarters | Yes | 23.02.2000 | 06.03.2000 |
| Navy | Yes | 12 01.2000 | 06.10.1999 |
| Army | Yes | 07.07.1998 | Noted by Inspector General[2] |
| Air Force | Yes | 01.12.1999 | 11.11.1999 |
| Intelligence | Yes | 31.04.2000 | 12.05.2000 |
| Support Command | Yes | 01.12.1999 | 14.12.1999 |
| Defence Personnel Executive | Yes | 03.03.2000 | 13.03.2000 |
| Acquisition | Yes | 02 05.2000 | 13.07.2000 |
| Science and Technology | Yes | 27.07.2000 | 08.08.2000 |
| Defence Estate | Yes | 15.11.1999 | 14.12.1999 |
| Defence Information Systems | Yes | 29.09.1999 | 06.10.1999 |
| Defence Corporate Support | No | 09.02.1999[3] | Not Endorsed |

Source: Inspector-General Division

1. The Group structure referred to in this table was amended on 1 July 2000.
2. The Army FCP was developed prior to the audit committee requirement of 17 September 1999.
3. Defence Corporate Support has developed a Business Rule. The Inspector-General has not endorsed this document as meeting the requirements of a Group fraud control plan.

## Sub-Group fraud control plans

**5.8** Defence's CEIs state that *'fraud control plans are to be developed to at least the Sub-Group level, and lower for some larger Sub-Groups.'*[67] This requirement is also set out in the DFCP3.[68]

**5.9** The ANAO found that only about 53 per cent of Sub-Group fraud control plans had been developed at the time of the audit fieldwork. Only one Group had all of its Sub-Group plans. This was two years after the promulgation of DFCP3. The situation in each Group is set out in Table 5.2.[69]

---

67 CEIs, Paras 117.

68 Defence Fraud Control Plan No.3, Figure 1.

69 The Group and Sub-Group structures referred to in this table were amended on 1 July 2000.

**Table 5.2**
**Sub-Group fraud control plans**

| *Group* | *Number of Sub-Groups* | *Number of Sub-Groups with plans* |
|---|---|---|
| Defence Headquarters | 14 | 1 |
| Navy | 3 | 0 |
| Army | 3 | 1 |
| Air Force | 3 | 2 |
| Intelligence | 3 | 0 |
| Support Command | 7 | 7 |
| Defence Personnel Executive | 6 | 3 |
| Acquisition | 20 | 15 |
| Science and Technology | 3 | 0 |
| Defence Estate | 4 | 0 |
| Defence Information Systems | 4 | 0 |
| Defence Corporate Support | 19 | 18 |
| **Total** | **89** | **47** |

Source: Management progress reports – DFCP3 (May/June 2000)

**5.10** The lack of fraud control plans has been raised as an issue by a number of Management Audit Branch reports.

**5.11** Many of the Group Coordinators informed the ANAO that they considered that their Group was not required to develop fraud control plans below the Group level. For instance, in the Intelligence Group it was decided that there was no need for fraud control plans below the Group level. The basis for this decision was that procurement and financial administrative support for the Intelligence Group (ie. Defence Intelligence Organisation, Australia Imagery Organisation and Defence Signals Directorate) is provided by the Executive Branch in Defence Signals Directorate.

**5.12** Non-compliance by two Groups (Defence Headquarters and Intelligence) with the requirement of the DFCP3 to have Sub-Group plans has the approval of the Inspector-General Division on the basis of effective and efficient use of resources. If Defence considers that plans need not be developed at some levels of particular Groups, such a position should be reflected in the Defence fraud control plan.

## Performance indicators

**5.13** For any management or administrative activity, performance indicators are needed to enable a designated entity to be accountable for taking particular action or delivering particular services to a specified standard. The indicators must also allow for cost-effective assessment

of the achievement of the particular action to the measurable standard. Such a standard could involve a time limit, budget and/or specified quality.

**5.14** Defence's three levels of fraud control plans refer to specific action to be taken to address identified risks and they give designated officers responsibility for carrying out that action and achieving results. However, the vast majority of performance indicators in the fraud control plans do not allow for regular assessment of their achievement. Examples of this include particular actions that are to be completed within timetables defined as *continuing*; *ongoing*; and *as required*. Fraud control plans should contain performance indicators that would allow regular assessment of progress in implementing them.

## Conclusion

**5.15** Many areas in Defence have not given sufficient priority to fraud control. The ANAO reviewed Defence's three levels of fraud control plans and found that many areas within Defence have not developed plans. Defence must ensure timely development of all fraud control plans that are required to be developed under the Defence fraud control plan.

**5.16** Most of the performance indicators included in Defence fraud control plans, at all three levels, are not measurable. Qualitative assessment in some aspects of fraud control is important, but a lack of measurable indicators inhibits a sound performance assessment process from operating within Defence in respect of fraud control.

## Recommendation No.4

**5.17** The ANAO *recommends* that Defence:

a) ensure timely completion of all Group, Unit and Project fraud control plans required by the Defence fraud control plan; and

b) include performance indicators in all Defence fraud control plans that allow regular assessment of progress.

*Defence response*

1.1 a) Agree.

b) Agree.

# 6. Defence Ethics and Fraud Awareness

*This Chapter examines various aspects of the operations of the Directorate of Fraud Control Policy and Ethics. Recommendations are made concerning scheduling of awareness sessions and monitoring of session attendance.*

**6.1** Fraud control education aims to help prevent and control fraud by raising the level of fraud awareness among staff. The Directorate of Fraud Control Policy and Ethics is responsible for managing the Defence ethics and fraud awareness campaign.

**6.2** The ANAO examined key aspects of the Directorate's operations, campaign staffing, scheduling of ethics and fraud awareness sessions and monitoring of session attendance.

## Staffing level

**6.3** Each year only about eight per cent of Defence employees attend ethics and fraud awareness sessions conducted by the Directorate. At the time of audit, it had one staff member engaged full-time on the ethics and fraud awareness campaign.[70] Three other staff members delivered ethics and fraud awareness sessions on a part-time basis as required.

**6.4** In addition to the Directorate's ethics and fraud awareness sessions, several Groups conduct their own ethics and fraud awareness training through their training areas and by the use of other in-house staff or external contractors.

**6.5** The development of fraud control plans for the Groups and Sub-Groups, and in some cases below these levels, has focused the attention of many managers on the need for ethics and fraud awareness education. Most Groups saw the Directorate's sessions as useful, especially as the Directorate was willing to tailor them to the target audience. The demand for sessions was evident among the Group staff interviewed as part of the audit. In fact, the ANAO's interviews resulted in about fifty inquiries to the Directorate concerning ethics and fraud awareness sessions.

[70] This position became vacant at the end of July 2000.

**6.6** The present staffing level would appear to be inadequate to cope with the expected increased demand for ethics and fraud awareness sessions. Defence can meet this increased level of demand in a number of ways. Options available to Defence would include:

- increasing the number of staff providing ethics and fraud awareness sessions;
- including the education of staff in fraud related matters in the general staff training arrangements; and
- engaging consultants to deliver ethics and fraud awareness courses.

**6.7** If the last two options were adopted, advice on course content and other support from the Directorate would be valuable.

## Scheduling

**6.8** The Directorate's schedule for managing its ethics and fraud awareness sessions is demand driven. Some presentations are provided at about the same time every year for certain areas of Defence such as military schools. Bookings for all other presentations are taken a few weeks in advance.

**6.9** A number of Group and Sub-Group fraud control plans state that various categories of personnel will attend ethics and fraud awareness sessions each year. A scheduling system for these sessions would allow Inspector-General Division to make medium and long-term resourcing decisions in respect of the Directorate. It would also allow Inspector-General Division to assess whether Groups or Sub-Groups would achieve their session attendance targets in the life of their fraud control plan.

## Ethics and fraud awareness session register

**6.10** The Directorate provides ethics and fraud awareness sessions but does not maintain a register of the personnel who have attended the sessions. It records the number but not the names of personnel who attend from specific areas in Defence. Discussion with the Groups indicates that, although registers are maintained at some training establishments, most Groups do not keep information on personnel who have attended ethics and fraud awareness sessions. Therefore no mechanism exists to show which Defence personnel have attended these sessions.

**6.11** The development of formal arrangements to monitor attendance at ethics and fraud awareness sessions would enable managers to ensure their staff have attended these sessions and that targets developed for their fraud control plans are achieved. This is particularly important in Defence with its regular cycle of military personnel postings (transfers).

## Conclusion

**6.12** Defence should prepare for an increase in demand for ethics and fraud awareness sessions that is expected to result from development of fraud control plans at the Group and Sub-Group level. This planning process has drawn many managers' attention to the need for such education and training. A system of scheduling ethics and fraud awareness sessions is required in the Directorate of Fraud Control Policy and Ethics to assist in forming medium and long-term resourcing decisions.

**6.13** Formal arrangements to monitor staff attendance at ethics and fraud awareness sessions would help to assess compliance with the requirements of the various fraud control plans, at all levels, for staff to attend such sessions and take appropriate action.

## Recommendation No.5

**6.14** The ANAO *recommends* that Defence develop:

a) scheduling arrangements for the ethics and fraud awareness sessions to allow better medium and long-term resourcing decisions to be made in the Inspector-General Division; and

b) formal arrangements to monitor staff attendance at ethics and fraud awareness sessions.

### *Defence response*

**6.15**

a) Agree, noting that the number of presentations is expected to reduce as other methods of delivery are introduced (for example, the use of the ethics website).

b) Agree. Responsibility for monitoring staff exposure to ethics and fraud awareness material remains with the unit commander or area manager. This information is a requirement in the half-yearly fraud control reporting provided to the Defence Audit Committee by the Inspector General.

# 7. Fraud Investigations

*This Chapter examines aspects of fraud investigation arrangements in Defence. Recommendations are made concerning development of consolidated and uniform procedures for Defence fraud investigations and competency standards for military personnel primarily engaged in investigating fraud.*

**7.1** The Directorate of Fraud Investigations and Recovery in Inspector-General Division undertakes all civilian fraud investigations and the more significant cases involving military personnel. The three military police services investigate the remaining military fraud incidents. The fraud investigations handled by the military police amount to 85 per cent of all fraud cases in Defence.

**7.2** Most prosecutions are pursued under the *Crimes Act 1914*, the *Defence Force Discipline Act 1982*, the *Public Service Act 1999* and State civil law. Indicative Inspector-General Division fraud investigation statistics for 1999–2000 are at Appendix 1.

**7.3** The ANAO examined key aspects of fraud investigation arrangements in Defence, including investigation guidelines, the fraud investigations database and competency training.

## Fraud investigation procedures

**7.4** A comprehensive set of procedures for the conduct of fraud investigations is necessary to provide direction to staff involved in fraud investigations. It assists in ensuring compliance with legislative and other requirements as well as effective and efficient operation of fraud investigative areas.

**7.5** As indicated above, four separate areas in Defence undertake fraud investigations. The ANAO found that each area uses a separate set of investigation guidelines. The Directorate of Fraud Investigations and Recovery uses a number of authority and guidance documents. Each of the three military police services' procedure manuals are consolidated documents but vary in the level of detail provided.

**7.6** The Directorate has been attempting to produce a Defence–wide consolidated procedures manual. The manual would assist in providing, among other benefits, a common classification system for cases under investigation and easier transfer of cases to the Directorate. Work on the manual has been underway for about eighteen months.

## Fraud investigations database

**7.7** In its 1991 report on Defence fraud control, the ANAO recommended that '*Defence develop and maintain a centralised database containing relevant details of all fraud allegations, investigations and outcomes*.' Defence accepted this recommendation and stated at the time that:

> *… the Inspector–General Division is about to trial a new database which is intended to consolidate the records of the Service police and the Inspector–General Division in a unified format. …*
>
> *The new database will allow management to access where historically, fraud has been the most prevalent and analyse any trends that are emerging in particular locations or activities.*[71]

**7.8** In 1999 Defence began development of a case management system for use by all investigative agencies in Defence. The system is expected to be operational by the end of 2000 and will facilitate analysis of fraud cases and the identification of trends.

**7.9** As discussed in Chapter 3, development of a sound fraud intelligence capacity to support the fraud risk assessment process would be assisted greatly by the existence of a linked investigation database. Groups have also informed the ANAO that the provision of more Defence-wide fraud control information would better inform their fraud control decision-making (refer Chapter 4). The ANAO encourages Defence to use the information from the new linked database for such purposes.

## Fraud investigation training

**7.10** The proposed new fraud control policy of the Commonwealth would provide that '*the Certificate IV, Fraud Control (Investigation) is the proposed competency standard required for personnel primarily engaged in the investigation of fraud.*'[72] Similar qualifications have been available for a number of years and, although not required previously, they are considered the minimum industry qualification.

---

[71] Audit Report No.15 1991-92 *Department of Defence – Procedures for Dealing with Fraud on the Commonwealth* pp56 and 57.

[72] Draft Fraud Control Policy of the Commonwealth, Fraud Control Guideline No.1, op. cit. This competency standard is established on the Australian National Training Register.

**7.11** The ANAO was informed that all fraud investigating staff in the Directorate of Fraud Investigations and Recovery have, or are obtaining, the Certificate IV qualification. However, the situation in relation to the military police is very different. The ANAO found that no military police in any of the three Services had the Certificate IV qualification. They have, however, undertaken other relevant training programs to assist them in undertaking their duties.

## Conclusion

**7.12** Completion of a Defence-wide consolidated procedures manual for fraud investigations will be fundamental in providing a common approach to investigation of fraud in Defence.

**7.13** Military police play a significant role in investigating fraud cases in Defence. It is important that the investigators have the appropriate competency qualifications.

## Recommendation No.6

**7.14** The ANAO *recommends* that Defence:

a) expedite the development of a consolidated and comprehensive set of fraud investigation procedures for Defence fraud investigations; and

b) ensure that military police undertaking fraud investigations have the competency standard required for personnel primarily engaged in the investigation of fraud.

*Defence response*

**7.15** a) Agree.

b) Agree, noting that it will take some time to implement.

---

Canberra ACT
14 December 2000

P. J. Barrett
Auditor-General

# Appendices

## Appendix 1

# Inspector-General Division fraud investigations

**1.** In the tables below are indicative figures for 1999–2000 relating to fraud investigations undertaken by Inspector-General Division. These represent approximately fifteen per cent of all Defence fraud investigations.

**2.** Defence indicated that the nature of the various fraud investigations databases did not allow it to supply information for the whole of Defence without a large expenditure of resources. Defence proposes to link the Inspector-General Division's investigations database with those of the military police in the three Services (refer Chapter 7). The new arrangements should have common definitions and allow fraud investigation information to be readily accessible.

### Table A1.1

**Types and number of cases investigated**

| *Case type* | *No. of cases* |
|---|---|
| Travel fraud | 11 |
| Abuse of office | 10 |
| Purchasing fraud | 9 |
| Abuse of resources | 5 |
| Pay fraud | 4 |
| Removal allowance fraud | 4 |
| Tender fraud | 3 |
| Compensation fraud | 3 |
| Theft | 3 |
| Conflict of interest | 2 |
| Improper disclosure of information | 2 |
| Rental allowance fraud | 2 |
| Corruption (in purchasing) | 2 |
| Disposal of assets fraud | 2 |
| Misconduct | 2 |
| Living allowance fraud | 1 |
| Misrepresentation | 1 |
| Cash Office fraud | 1 |
| Australian Government Credit Card fraud | 1 |
| Probity matter (Ministerial reference) | 1 |
| Other | 1 |
| **Total**[73] | **70** |

Source: Inspector-General Division

[73] These figures are indicative only and do not reflect the breakdown of one of the major cases into a number of smaller investigations.

## Table A1.2
**Outcome of investigations**

| *Outcome type* | *No. of cases* |
|---|---|
| Unfounded | 30 |
| Resolved by administrative action | 11 |
| Inconclusive | 11 |
| *Public Service Act* action—proven | 5 |
| *Crimes Act* convictions | 3 |
| Civil recovery successes | 3 |
| Discontinued investigations | 2 |
| Commonwealth Director of Public Prosecutions declined to prosecute | 2 |
| **Total** | **67** |

Source: Inspector-General Division

## Table A1.3
**Estimated value of cases at commencement of investigation**

| *Value range* | *No. of cases* |
|---|---|
| Nil value identified | 9 |
| Less than $1 000 | 4 |
| $1 000–$10 000 | 12 |
| $10 000–$50 000 | 7 |
| Greater than $50 000 | 3 |
| Unknown | 32 |

Source: Inspector-General Division

## Table A1.4
**Recovery of moneys**

| | |
|---|---|
| Number of cases | 10 |
| Losses currently awarded | $169 000 |

Source: Inspector-General Division

## Appendix 2

# Audit Survey of Fraud Arrangements in APS Agencies

The overall conclusion of Audit Report No.47 1999–2000 *Survey of Fraud Arrangements in APS Agencies* is set out below.

### Overall conclusion

**12.** The ANAO concluded that the majority of APS agencies had a framework in place which contained key elements for effectively preventing and dealing with fraud in line with Commonwealth Policy.

**13.** The extent of these arrangements ranged from the majority of agencies having undertaken fraud-awareness-raising activities, to a lesser proportion having specific fraud policies and fraud control plans in place and having undertaken risk assessments.

**14.** This clearly indicated that the majority of agencies took their responsibilities for fraud control seriously. However, in a number of areas a significant proportion of agencies did not have appropriate fraud control arrangements in place. A particular issue that the survey results highlighted was the fact that many agencies (about one third) had not undertaken a recent risk assessment to identify the existing risks and those emerging as a result of the changing environment and methods of service delivery.

**15.** For *Commonwealth Authorities and Companies* and *Financial Management and Accountability* (FMA) bodies this indicates a lack of adherence to the principles of sound corporate governance. As well, a number of agencies had not developed fraud control plans, of which seven were FMA bodies. The latter agencies were therefore not meeting the requirements under Section 45 of the FMA Act to have a fraud control plan. The ANAO has written separately to these agencies bringing this matter to their attention.

**16.** These gaps in governance arrangements have occurred despite a reported high level of awareness of the 1994 Fraud Control Policy of the Commonwealth (93 per cent). A lesser proportion of agencies (79 per cent) indicated awareness of the Consultation Draft. While the conduct of the ANAO survey may have served to raise the level of awareness of the Consultation Draft, agencies will need to heighten their awareness and take action to ensure that their future arrangements meet policy guidelines.

**17.** The survey highlighted that 85 per cent of fraud committed occurs in less than ten per cent of agencies. These agencies tended to be the ones with comprehensive fraud control systems in place. This does not mean that other agencies can assume an absence of fraud. It may only be that they have no systems to detect fraud or other losses to the Commonwealth.

**18.** The level of fraud reported for 1998–99 by agencies responding to the survey was $146 million. This figure must be seen as only the minimum level of fraud because varying definitions of fraud are used across the APS. In essence, the measurement of the actual level of fraud is difficult. As well, the nature of fraud is changing as the APS adopts new approaches to deliver government services and makes greater use of e-commerce, including the Internet. To allow for a better understanding of the type and scale of response required to control fraud, agencies will need to make greater efforts to clearly define (using the Fraud Control Policy definition wherever possible) and measure fraud.

## Appendix 3

# US GAO report on program risks in US Defense

*The following extracts referring to fraud risks are from US General Accounting Office (GAO) report* Major Management Challenges and Program Risks—Department of Defense *(January 1999) GAO/OCG–99–4.*

Long-standing weaknesses in DOD's [US Department of Defense] financial management operations continue to result in wasted resources, to undermine DOD's ability to manage an estimated $250 billion budget and $1 trillion in assets, and to limit the reliability of the financial information provided to the Congress…

DOD has not ensured that all disbursements were properly recorded and reconciled. Over the years, we and DOD auditors have reported that DOD'S payment processes and systems have serious internal control weaknesses that have resulted in numerous erroneous and in some cases fraudulent payments. For example, we recently reported that weak controls led to two fraud cases involving nearly $1 million in embezzled Air Force vendor payments and that similar control weaknesses continue to leave Air Force funds vulnerable to additional fraudulent and improper vendor payments…

In addition, to achieve the wide-ranging reforms necessary to address its long-standing financial management deficiencies, we have made numerous recommendations to DOD regarding its need to upgrade the skills of its financial personnel and successfully overcome serious design flaws in its financial systems. Until DOD deals with these two key issues, resolution of its financial management problems is unlikely…

Until DOD has developed integrated financial management systems, its operations will continue to be burdened with costly, error-prone systems without financial controls to ensure that DOD's assets are safeguarded, its resources appropriately accounted for, or the cost of its activities are accurately measured. Concerns continue over whether DOD (1) has comprehensively identified all the systems it relies on to carry out its financial management operations; (2) corrected weaknesses that would allow both hackers and hundreds of thousands of legitimate users with valid access privileges to modify, steal, inappropriately disclose, and destroy sensitive DOD data; and (3) effectively documented how it conducts its financial management operations now and plans to in the future…

DOD spends in excess of $100 billion a year contracting for goods and services. Since 1995, we have reported DOD contract management as a high-risk area, and it remains on our list of high-risk areas. Over the last few years, several broad-based changes have been made to DOD

acquisition and contracting processes to improve the way DOD relates to its contractors and the rules governing their relationships. And the changes are by no means complete…

Our work, and that of the DOD IG [Inspector-General], continue to identify risks in DOD contracting activity. For example, DOD continues to experience problems with erroneous, fraudulent, and improper payments to its contractors; paying higher prices for commercial spare parts than necessary; and awarding and administering its health care contracts…

The need for DOD to achieve effective control over its payment process remains an imperative. If it does not, DOD continues to risk erroneously paying contractors millions of dollars and perpetuating other financial management and accounting control problems…

DOD receives about a billion dollars a year in checks from defense contractors. While some of these are the result of contract changes that result in reduced prices, others represent errors by DOD'S payment center. DOD is conducting a demonstration program to evaluate the feasibility of using private contractors to identify overpayments made to vendors. Through this process, known as recovery auditing, the contractor has identified about 19 million in overpayments. DOD is examining opportunities to expand the use of recovery auditing, which we believe offers potential to identify overpayments…

In addition to erroneous payments, weak systems and internal controls can leave DOD vulnerable to fraud and improper payments. Our September l998 report discussed two cases of fraud that resulted from a weak internal control environment. The lack of segregation of duties and other control weaknesses, such as weak controls over remittance addresses, created an environment in which employees were given broad authority and the capability, without compensating controls, to perform functions that should have been performed by separate individuals under proper supervision…

The vulnerability of in-transit inventory to waste, fraud, and abuse is another area of concern. In February 1998 we reported that DOD did not have receipts for about 60 percent of its 21 million shipments to end users in fiscal year 1997. Later work shows that, over the last 3 years, the Navy alone reportedly wrote off as lost over $3 billion in in-transit inventory. The vulnerability to waste, fraud, and abuse also extends to DOD'S disposal of surplus property. In October 1997, we reported that DOD destroyed and sold as scrap some useable aircraft parts in new or repairable condition that could have been sold intact at higher than scrap prices. In contrast, in August 1998, we reported that DOD inadvertently sold surplus parts with military technology intact.

## Appendix 4

# Performance audits in Defence

*Set out below are the titles of the ANAO's previous performance audit reports on the Department of Defence and the Australian Defence Force (ADF) tabled in the Parliament in the last six years.*

Audit Report No.8 1995–96
*Explosive Ordnance* (follow-up audit)

Audit Report No.11 1995–96
*Management Audit*

Audit Report No.17 1995–96
*Management of ADF Preparedness*

Audit Report No.26 1995–96
*Defence Export Facilitation and Control*

Audit Report No.28 1995–96
*Jindalee Operational Radar Network Project [JORN]*

Audit Report No.31 1995–96
*Environmental Management of Commonwealth Land*

Audit Report No.15 1996–97
*Food Provisioning in the ADF*

Audit Report No.17 1996–97
*Workforce Planning in the ADF*

Audit Report No.27 1996–97
*Army Presence in the North*

Audit Report No.34 1996–97
*ADF Health Services*

Audit Report No.5 1997–98
*Performance Management of Defence Inventory*

Audit Report No.34 1997–98
*New Submarine Project*

Audit Report No.43 1997–98
*Life-cycle Costing in Defence*

Audit Report No.2 1998–99
*Commercial Support Program*

Audit Report No.17 1998–99
*Acquisition of Aerospace Simulators*

Audit Report No.41 1998–99
*General Service Vehicle Fleet*

Audit Report No.44 1998–99
*Naval Aviation Force*

Audit Report No.46 1998–99
*Redress of Grievances in the ADF*

Audit Report No.13 1999–00
*Management of Major Equipment Acquisition Projects*

Audit Report No.26 1999–00
*Army Individual Readiness Notice*

Audit Report No.35 1999–00
*Retention of Military Personnel*

Audit Report No.37 1999–00
*Defence Estate Project Delivery*

Audit Report No.40 1999–00
*Tactical Fighter Operations*

Audit Report No.41 1999–00
*Commonwealth Emergency Management Arrangements*

Audit Report No.50 1999–00
*Management Audit Branch—Follow-up*

Audit Report No.3 2000–01
*Environmental Management of Commonwealth Land—follow-up*

Audit Report No.8 2000–01
*Amphibious Transport Ship Project*

Audit Report No.11 2000–01
*Knowledge System Equipment Acquisition Projects in Defence*

## Appendix 5

# Previous ANAO performance audits on agency fraud control arrangements

*Set out below are the titles of the ANAO's previous performance audit reports on the agency fraud control arrangements tabled in the Parliament in the last decade.*

Audit Report No.25 1990–91
*Efficiency and Effectiveness of Fraud Investigations*
Australian Federal Police

Audit Report No.15 1991–92
*Procedures for Dealing with Fraud on the Commonwealth*
Department of Defence

Audit Report No.40 1991–92
*Systems for the Detection of Overpayments and the Investigation of Fraud*
Department of Social Security

Audit Report No.11 1992–93
*Procedures for Dealing with Fraud on the Commonwealth*
Department of Administrative Services

Audit Report No.31 1996–97
*Medifraud and Inappropriate Practice*
Health Insurance Commission

Audit Report No.4 1999–00
*Fraud Control Arrangements in Employment, Education, Training and Youth Affairs*
Department of Employment, Education, Training and Youth Affairs

Audit Report No.47 1999–00
*Survey of Fraud Arrangements in APS Agencies*

Audit Report No.5 2000–01
*Fraud Control Arrangements in the Department of Industry, Science and Resources*
Department of Industry, Science and Resources

Audit Report No.6 2000–01
*Fraud Control Arrangements in the Department of Health and Aged Care*
Department of Health and Aged Care

Audit Report No.16 2000–01
*Internal Fraud Control Arrangements*
Australian Taxation Office

# Index

# Series Titles

## Titles published during the financial year 2000–01

Audit Report No.20 Performance Audit
*Second Tranche Sale of Telstra Shares*

Audit Report No.19 Financial Control and Administration Audit
*Management of Public Sector Travel Arrangements—Follow-up audit*

Audit Report No.18 Performance Audit
*Reform of Service Delivery of Business Assistance Programs*
Department of Industry, Science and Resources

Audit Report No.17 Performance Audit
*Administration of the Waterfront Redundancy Scheme*
Department of Transport and Regional Services
Maritime Industry Finance Company Limited

Audit Report No.16 Performance Audit
*Australian Taxation Office Internal Fraud Control Arrangements*
Australian Taxation Office

Audit Report No.15 Performance Audit
*Agencies' Performance Monitoring of Commonwealth Government Business Enterprises*

Audit Report No.14 Information Support Services Report
*Benchmarking the Internal Audit Function*

Audit Report No.13 Performance Audit
*Certified Agreements in the Australian Public Service*

Audit Report No.12 Performance Audit
*Passenger Movement Charge—Follow-up Audit*
Australian Customs Service

Audit Report No.11 Performance Audit
*Knowledge System Equipment Acquisition Projects in Defence*
Department of Defence

Audit Report No.10 Performance Audit
*AQIS Cost-Recovery Systems*
Australian Quarantine and Inspection Service

Audit Report No.9 Performance Audit
*Implementation of Whole-of-Government Information Technology Infrastructure Consolidation and Outsourcing Initiative*

Audit Report No.8 Performance Audit
*Amphibious Transport Ship Project*
Department of Defence

Audit Report No.7 Performance Audit
*The Australian Taxation Offices' Use of AUSTRAC Data*
Australian Taxtion Office

Audit Report No.6 Performance Audit
*Fraud Control Arrangements in the Department of Health & Aged Care*
Department of Health & Aged Care

Audit Report No.5 Performance Audit
*Fraud Control Arrangements in the Department of Industry, Science & Resources*
Department of Industry, Science & Resources

Audit Report No.4 Activity Report
*Audit Activity Report: January to June 2000—Summary of Outcomes*

Audit Report No.3 Performance Audit
*Environmental Management of Commonwealth Land—Follow-up audit*
Department of Defence

Audit Report No.2 Performance Audit
*Drug Evaluation by the Therapeutic Goods Administration—Follow-up audit*
Department of Health and Aged Care
Therapeutic Goods Administration

Audit Report No.1 Performance Audit
*Commonwealth Assistance to the Agrifood Industry*

# Better Practice Guides

| | |
|---|---|
| AMODEL Illustrative Financial Statements 2000 | Apr 2000 |
| Business Continuity Management | Jan 2000 |
| Building a Better Financial Management Framework | Nov 1999 |
| Building Better Financial Management Support | Nov 1999 |
| Managing APS Staff Reductions (in Audit Report No.47 1998–99) | Jun 1999 |
| Commonwealth Agency Energy Management | Jun 1999 |
| Corporate Governance in Commonwealth Authorities and Companies–Principles and Better Practices | Jun 1999 |
| Managing Parliamentary Workflow | Jun 1999 |
| Cash Management | Mar 1999 |
| Management of Occupational Stress in Commonwealth Agencies | Dec 1998 |
| Security and Control for SAP R/3 | Oct 1998 |
| Selecting Suppliers: Managing the Risk | Oct 1998 |
| New Directions in Internal Audit | Jul 1998 |
| Life-cycle Costing (in Audit Report No.43 1997–98) | May 1998 |
| Controlling Performance and Outcomes | Dec 1997 |
| Management of Accounts Receivable | Dec 1997 |
| Protective Security Principles (in Audit Report No.21 1997–98) | Dec 1997 |
| Public Sector Travel | Dec 1997 |
| Audit Committees | Jul 1997 |
| Core Public Sector Corporate Governance (includes Applying Principles and Practice of Corporate Governance in Budget Funded Agencies) | Jun 1997 |
| Administration of Grants | May 1997 |
| Management of Corporate Sponsorship | Apr 1997 |
| Return to Work: Workers Compensation Case Management | Dec 1996 |
| Telephone Call Centres | Dec 1996 |
| Telephone Call Centres Handbook | Dec 1996 |
| Paying Accounts | Nov 1996 |
| Performance Information Principles | Nov 1996 |
| Asset Management | Jun 1996 |
| Asset Management Handbook | Jun 1996 |
| Managing APS Staff Reductions | Jun 1996 |