The Parliament of the Commonwealth of Australia

Report 385

- **Australian Taxation Office Internal Fraud Control Arrangements**
- **Fraud Control in Defence**
- **Defence Estate Facilities Operations**

Review of Auditor-General's Reports
2000–2001
Second & Third Quarters

Joint Committee of Public Accounts and Audit

August 2001
Canberra

ISBN [Click **here** and type ISBN Number]

Contents

APPENDICES

Foreword

Report 385 is the outcome of the review by the Joint Committee of Public Accounts and Audit (JCPAA) of the Auditor-General's audit reports tabled in the second and third quarters of 2000–2001. Of the eighteen audit reports reviewed, the Committee selected three for further examination.

Audit Report No.16, *Australian Taxation Office Internal Fraud Control Arrangements;* Audit Report No.22, *Fraud Control in Defence*; and Audit Report No. 26, *Defence Estate Facilities Operations* were examined at public hearings in Canberra on Friday, 2 May 2001.

The ANAO has undertaken a series of performance audits on fraud control following the 1994 formation of the Commonwealth Law Enforcement Board to co-ordinate and develop public sector fraud control policy and to support the systemic commitment to eliminating fraudulent activity. The Committee is aware that the Attorneys-General have been working with agencies to reach an agreed definition of fraud. The Committee considers it would be useful for the ANAO, in its preparation of a better practice guide on fraud control, to develop subcategories of fraud for the purposes of fraud reporting, and has recommended accordingly.

Audit Report No 16 focused on internal fraud prevention and control arrangements in the Australian Taxation Office (ATO). The ANAO found that the ATO had demonstrated a strong commitment to fraud control and had established a comprehensive fraud control policy framework. The ANAO also found that the level of alleged fraud had steadily increased in recent years and that the security of IT systems should be an ongoing concern to ATO management.

Audit Report No. 22 examined the strategies developed by the Department of Defence for sound fraud control arrangements. ANAO found that there was scope for improvement in Defence's corporate governance with reference to fraud control. For instance, Defence's *Chief Executive Instructions* did not comply with the Commonwealth fraud control policy requirement to review its fraud control arrangements every two years. The

audit found that Defence lacked a suitable fraud intelligence capability, thereby making it difficult for Defence to estimate accurately the extent of fraud in or against Defence.

Although the Committee accepts that the amount of fraud detected in Defence has been fairly consistent over the past five years, the Committee questions whether Defence has been as diligent as it could be in detecting fraud, given that its asset register 'is not in good shape' and fraud investigation is undertaken in four separate areas. Namely the Inspector-General's division and the military police in each of the services.

The Committee is not convinced that the financial and administrative systems Defence has in place are sufficient to obtain an adequate organisational view of the occurrence of fraud in Defence. The Committee recommends that Defence address the shortcomings in its asset registers and develop a fraud intelligence capability.

Audit Report No. 26 was undertaken by ANAO to assess the efficiency and effectiveness of selected Defence facilities operations with a view to making practical recommendations for enhancing operations. The Committee was told that Defence Estate Office (DEO) had made a significant effort to develop and implement a strategic, corporate-focused framework for the delivery of maintenance work through its FACOPS Program. Initiatives, such as the Comprehensive Maintenance Contract, focus on economies and efficiencies that earlier approaches and/or methods lacked.

Evidence showed that DEO staff need to develop their abilities to prioritise timely maintenance, develop sound business practices and the skills to manage contractors. Defence needs to hone its performance indicators to reflect these skills and implement appropriate staff replacement strategies.

Having considered the evidence, the Committee believes that Defence still has a problem regarding its asset and property registers. While the Committee acknowledges that Defence is making an effort to achieve a full register and link it to ROMANS, the Committee is not satisfied that all the problems have been addressed effectively.

The Committee is aware of Defence's poor record in contract and project management, and is of the view that Defence still has a long way to go before DEO staff are able to effectively exercise their responsibilities for properties and assets with a gross replacement value of $14.8 billion.

Bob Charles MP
Chairman

Membership of the Committee

Chair Mr Bob Charles MP

Deputy Chair Mr David Cox MP

Members

Senator Helen Coonan

Senator the Hon Rosemary Crowley (until 28/06/01)

Senator the Hon John Faulkner (until 12/10/00)

Senator the Hon Brian Gibson AM

Senator John Hogg

Senator Andrew Murray

Senator the Hon Nick Sherry (from 28/06/01)

Senator John Watson

Mr Kevin Andrews MP

Mr Malcolm Brough MP (until 7/3/00)

Mr Petro Georgiou MP

Ms Julia Gillard MP

Mr Alan Griffin MP (until 9/8/99)

Mr Peter Lindsay MP (from 7/3/00)

Ms Tanya Plibersek MP (until 10/4/00)

The Hon Alex Somlyay MP

Mr Stuart St Clair MP

Mr Lindsay Tanner MP (from 9/8/99)

Mr Kelvin Thomson MP (from 10/4/00)

Membership of the Sectional Committee

Chair	Mr Bob Charles MP	
Deputy Chair	Mr David Cox MP	
Members	Mr Petro Georgiou MP	Senator the Hon Brian Gibson AM
	Ms Julia Gillard MP	Senator Andrew Murray
	Mr Peter Lindsay MP	
	Mr Alex Somlyay MP	
	Mr Lindsay Tanner MP	

Committee Secretariat

Secretary	Dr Margot Kerley
Inquiry staff	Ms Maureen Chan
	Mr Stephen Boyd
	Ms Jennifer Hughson
	Mr Ngan Thai
	Ms Maria Pappas

Duties of the Committee

The Joint Committee of Public Accounts and Audit is a statutory committee of the Australian Parliament, established by the *Public Accounts and Audit Committee Act 1951*.

Section 8(1) of the Act describes the Committee's duties as being:

(a) to examine the accounts of the receipts and expenditure of the Commonwealth, including the financial statements given to the Auditor-General under subsections 49(1) and 55(2) of the *Financial Management and Accountability Act 1997*;

(b) to examine the financial affairs of authorities of the Commonwealth to which this Act applies and of inter-governmental bodies to which this Act applies;

(c) to examine all reports of the Auditor-General (including reports of the results of performance audits) that are tabled in each House of the Parliament;

(d) to report to both Houses of the Parliament, with any comment it thinks fit, on any items or matters in those accounts, statements and reports, or any circumstances connected with them, that the Committee thinks should be drawn to the attention of the Parliament;

(e) to report to both Houses of the Parliament any alteration that the Committee thinks desirable in:
   (i) the form of the public accounts or in the method of keeping them;or
   (ii) the mode of receipt, control, issue or payment of public moneys;

(f) to inquire into any question connected with the public accounts which is referred to the Committee by either House of the Parliament, and to report to that House on that question;

(g) to consider:
  (i) the operations of the Audit Office;
  (ii) the resources of the Audit Office, including funding, staff and information technology;
  (iii) reports of the Independent Auditor on operations of the Audit Office;

(h) to report to both Houses of the Parliament on any matter arising out of the Committee's consideration of the matters listed in paragraph (g), or on any other matter relating to the Auditor-General's functions and powers, that the Committee considers should be drawn to the attention of the Parliament;

(i) to report to both Houses of the Parliament on the performance of the Audit Office at any time;

(j) to consider draft estimates for the Audit Office submitted under section 53 of the *Auditor-General Act 1997*;

(k) to consider the level of fees determined by the Auditor-General under subsection 14(1) of the *Auditor-General Act 1997*;

(l) to make recommendations to both Houses of Parliament, and to the Minister who administers the *Auditor-General Act 1997*, on draft estimates referred to in paragraph (j);

(m) to determine the audit priorities of the Parliament and to advise the Auditor-General of those priorities;

(n) to determine the audit priorities of the Parliament for audits of the Audit Office and to advise the Independent Auditor of those priorities; and

(o) any other duties given to the Committee by this Act, by any other law or by Joint Standing Orders approved by both Houses of the Parliament.

List of abbreviations

ADF	Australian Defence Force
AFP	Australian Federal Police
ANAO	Australian National Audit Office
APS	Australian Public Service
ATO	Australian Taxation Office
CEIs	Chief Executive Instructions
CLEB	Commonwealth:Law Enforcement Board
CMC	Comprehensive Maintenance Contract
DAC	Defence Audit Committee
DEO	Defence Estate Organisation
DEMS	Defence Estate Management System
DEMS/FM	Defence Estate Management System—Facilities Maintenance
DOD	[USA] Department of Defence
DoFA	Department of Finance and Administration
DPP	Director of Public Prosecutions
EDS	Electronic Data Systems
EOP	Estate Operations and Planning Branch

FACOPS	Facilities Operations
FP&C	Fraud Prevention and Control
IT	Information Technology
JCPAA	Joint Committee of Public Accounts and Audit
LANs	Local area networks
RECs	Regional Estate Centres
SDSS	Standard Defence Supply System
WAN	Wide Area Network

List of recommendations

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

Recommendation 1 [paragraph 2.26]

The Committee recommends that the ANAO, in its preparation of a better practice guide on fraud control, develop subcategories of fraud for the purposes of fraud reporting, and discuss this issue with the Joint Committee of Public Accounts and Audit prior to finalisation of the better practice guide.

Audit Report No.22, *Fraud Control in Defence*

Recommendation 2 [paragraph 3.53]

The Joint Committee of Public Accounts and Audit recommends the Department of Defence address the shortcomings in its asset registers and report back to the Committee on the condition of its asset registers in July 2002.

Audit Report No.22, *Fraud Control in Defence*

Recommendation 3 [paragraph 3.68]

The Joint Committee of Public Accounts and Audit recommends that the Department of Defence immediately implement the Australian National Audit Office recommendation that it develop a fraud intelligence capability to ensure better management of public funds and increase its ability to detect fraudulent activity in Defence.

Audit Report No.26, *Defence Estate Facilities Operations*

Recommendation 4 [paragraph 4.40]

The Committee recommends that the Defence Estate Organisation facilitate the consolidation of Regional Estate Centre activities fully onto Defence Estate Management System.

Audit Report No.26, *Defence Estate Facilities Operations*

Recommendation 5 [paragraph 4.64]

The Committee recommends that Defence review its performance indicators for Defence Estate Organisation staff so that staff are encouraged to develop essential management and financial skills.

1

Introduction

1.1 One of the statutory duties of the Joint Committee on Public Accounts and Audit (JCPAA) is to examine all reports of the Auditor-General in terms of the significance of the program or issues raised; the significance of the findings; the arguments advanced by the audited agencies; and the nature of public interest in the report. The Committee is then required to report the results of its deliberations to both Houses of Parliament as it sees fit.

1.2 Upon consideration of the eighteen audit reports presented to the Parliament by the Auditor-General during the second and third quarters of 2000–2001, the JCPAA selected three reports for further scrutiny at public hearings. The public hearings were conducted in Canberra on Wednesday, 2 May 2001.

1.3 The reports selected were:

- **Audit Report No.16,** ***Australian Taxation Office Internal Fraud Control Arrangements,*** Australian Taxation Office;
- **Audit Report No.22,** ***Fraud Control in Defence,*** Department of Defence; and
- **Audit Report No. 26,** ***Defence Estate Facilities Operations,*** Department of Defence.

Structure of the Report

1.4 This report draws attention to the main issues raised at the public hearing. Where appropriate, the Committee has commented on unresolved or contentious issues.

1.5 Chapter 2 of the report discusses the evidence taken relating to Audit Report No. 16, *Australian Taxation Office Internal Fraud Control Arrangements.* The Committee discusses the definition of fraud, fraud control and IT security.

1.6 Chapter 3 of the report addresses issues raised in relation to Audit Report No. 22, *Fraud Control in Defence,* such as Defence's management of fraud control and detection and the extent instances of fraud have been detected. The Committee found that Defence's incomplete asset register makes it difficult for fraud control and detection.

1.7 Chapter 4 of the report discusses the evidence taken relating to Audit Report No. 26, *Defence Estate Facilities Operations,* on management of properties and assets by the Defence estate Organisation. The Committee discusses its concerns about contract management; staff recruitment, retention and training; financial management; and the sale and lease-back of Defence estate.

1.8 In addition, the report provides an outline of the conduct of the Committee's review (Appendix A). The report should be read in conjunction with the transcript of evidence collected at the public hearing (Appendix C).

Report

1.9 A copy of this report is available on the JCPAA website at *http://www.aph.gov.au/house/committee/ jpaa/reports.htm*

2

Audit Report No. 16, 2000-2001

Australian Taxation Office Internal Fraud Control Arrangements

Australian Taxation Office

Introduction

Background

2.1 The prevention and detection of fraud within the Commonwealth public sector is not only important to protect Commonwealth revenue, expenditure and property, but also to maintain the Parliament's and community's confidence in the staff and operations of public sector agencies.

2.2 The Commonwealth Government first made a coordinated and systematic commitment to the prevention of fraud across the Australian Public Service (APS) in 1987 when the government released *The Fraud Control Policy of the Commonwealth.* Fraud is defined in this policy as:

> …inducing a course of acting or deceit involving acts or omissions or the making of false statement orally or in writing with the object of obtaining money or other benefit from, or evading liability to, the Commonwealth.[1]

---

1 ANAO, Audit Report No. 16, *Australian Taxation Office Internal Fraud Control Arrangements,* 2000–2001, Commonwealth of Australia, p. 31.

2.3 In 1994, the Government formed the Commonwealth Law Enforcement Board (CLEB) to ensure that all Commonwealth agencies with law enforcement responsibilities were able to adapt to the changing criminal environment and work together to pursue the Government's law enforcement interests. As part of its mission, CLEB[2] had responsibility for the coordination and development of public sector fraud control policy, as well as overseeing the implementation and maintenance of this policy within Commonwealth agencies.[3]

2.4 The Commonwealth Fraud Control Policy was developed further in 1994. The objectives of the Commonwealth Fraud Control Policy are to:

- protect public money and property;
- protect the integrity, security and reputation of public institutions; and
- maintain high levels of service to the community consistent with the good Government of the Commonwealth.

2.5 The Attorney-General's Department is continuing the development of these objectives in three main areas, namely:

- the reduction of losses through fraud by the rigorous implementation of fraud prevention procedures;
- a commitment to a policy of detection, investigation and prosecution of individual cases of fraud; and
- respect for the civil rights of all citizens.[4]

2.6 A review by the Attorney-General's Department of the Commonwealth Fraud Control Policy led to the release of *The Fraud Control Policy of the Commonwealth, Consultation Draft No. 1* in June 1999 and, in April 2001, the release of *Commonwealth Fraud Control Policy and Guidelines, Consultation Draft No. 2.*

2.7 The Government has outlined in this policy that responsibility for its implementation and for administration of fraud control rests with each Commonwealth agency and, more particularly, the Chief Executives of those agencies.[5]

---

2 The functions ascribed to CLEB are now being carried out by the Attorney-General's Department and the Australian Federal Police.

3 ANAO, Audit Report No. 16, 2000-2001, p. 31.

4 ANAO, Audit Report No. 16, 2000-2001, p. 32.

5 Attorney-General's Department, *Commonwealth Fraud Control Policy and Guidelines, Consultation Draft No. 2,* April 2001, pp.1-2.

ANAO objective and findings

2.8 In Audit Report No. 16, 2000–2001, *Australian Taxation Office Internal Fraud Control Arrangements*, the objective of the audit was to assess the administration of internal fraud control arrangements in the Australian Taxation Office (ATO) and to identify areas with potential for improvement.[6]

2.9 The audit focused on the ATO's internal fraud prevention and control arrangements. In particular, the audit looked at the activities of the Fraud Prevention and Control (FP&C) Section, corporate governance processes (including risk management) and ATO Business Line involvement in preventing and detecting internal fraud.[7]

2.10 The ANAO found that:

- the ATO had demonstrated a strong commitment to comprehensive fraud control by investing significant resources in establishing and supporting fraud prevention and control capability and creating an ethical workplace culture and environment;
- the ATO had established a comprehensive fraud control policy framework;
- the level of alleged fraud in the ATO had steadily increased over the last few years;
- the security of IT systems should be an ongoing concern to ATO management; and
- the security of its Fraud Prevention Case Management System could be enhanced.[8]

2.11 The ANAO made 11 recommendations to improve the administration of internal fraud control arrangements in the ATO. The ATO agreed to all of the recommendations.

2.12 The ATO advised the Joint Committee of Public Accounts and Audit (JCPAA) that it expected to have the majority of the ANAO's recommendations implemented by the end of the calendar year.[9]

6 ANAO, Audit Report No. 16, 2000-2001, p. 38.
7 ANAO, Audit Report No. 16, 2000-2001, p. 39.
8 ANAO, Audit Report No. 16, 2000-2001, pp. 15-16.
9 A Preston, *Transcript*, 2 May 2001, p. 3.

Issues discussed at the public hearing

2.13 In the course of the public hearing, the JCPAA took evidence on the following:

- the definition of 'fraud';
- fraud control framework;
- private binding rulings;
- fraud prevention, and
- IT security.

Definition of 'fraud'

2.14 The audit report noted that the level of alleged fraud reported in the ATO has steadily increased over the last few years.

2.15 The dollar value of reported internal fraud is not readily available. Prior to 1998-99, the Fraud Prevention and Control (FP&C) Section estimated the value of assets lost to internal fraud and the dollar amount recovered. However, the ATO has advised that it now considers that these figures were indicative, cannot be substantiated and are of minimal relevance. For the ATO, maintaining community confidence and minimising fraud were the driving factors rather than the monetary amount of the fraud.[10]

2.16 Unauthorised access to taxpayer data remains the most common type of fraud perpetrated in the ATO.

2.17 The Committee asked the ATO how many of the 373 alleged cases of fraud reported in 1999-2000 were accessing a taxation file with the intent of blackmail or sale of information, or placing a contract with a supplier in return for money.[11]

2.18 An ATO spokesperson told the Committee:

> I am not aware of any cases in the last couple of years that fall into the categories that you have just mentioned.…About 60 per cent of our cases [of fraud]

10 ANAO, Audit Report No. 16, 2000-2001, p. 36.

11 *Transcript*, 2 May 2001, p. 4.

> centre on unauthorised use of our computer systems to access taxpayer information.
>
> Our experience is that it is browsing and curiosity and acting in breach of the secrecy provisions in the various tax laws. We have no evidence of officers selling [information]. We have undertaken a number of investigations of staff who have been suspected of leaking information to the media for whatever purposes. But none of those enquiries have ever been able to substantiate to the required standard of proof that a particular individual committed the offence.[12]

2.19 The Committee raised the issue of the definition of 'fraud' with the ATO, asking whether it thought that the definition currently in place across the Commonwealth was a reasonable reflection of the common idea of fraudulent activity.[13]

2.20 The ATO responded that there had been a considerable degree of variation in the definition and it was now a service-wide issue to get a standardised definition:

> [The ATO puts] a very high focus on going beyond the purely quantitative direct harm [of fraud] to the Commonwealth in terms of revenues or expenditures and go to issues like inappropriate use of information, the influence value of gifts, and perception surrounding conflicts of interest. They are all intangibles, but they are of fundamental importance to an integrity based organisation.[14]

2.21 The Committee made the point that it attempted to promote widely greater accountability in the public sector, greater transparency, and reduction of fraud and criminality in dealings within the public sector and between the public and private sectors. It had some concern that other countries in the region may interpret the published fraud figures as representing what the Committee might term major fraud.[15]

---

12 R Mulligan, *Transcript*, 2 May 2001, p. 4.

13 *Transcript*, 2 May 2001, pp. 4-5.

14 Preston, *Transcript*, 2 May 2001, p. 5.

15 *Transcript*, 2 May 2001, p. 5.

2.22 The ATO indicated that it would not regard the published figures as an indicator of major fraud, but as an indicator of concern to the ATO:

> …I do not think I would interpret it as the source of concern in terms of our international credibility.[16]

2.23 The Committee asked whether there was a risk of encouraging fraud by talking about it so much, and whether there might be a need to change the language so that the highest ethical standards were encouraged in employees and contractors.[17]

2.24 The ATO was sympathetic to the Committee's view and noted that it was trying to transform the culture into a general focus on integrity in the broader context, within which the specific incidence of fraud was dealt with.[18]

Committee comments

2.25 While the Committee agrees with the ATO that unauthorised access to taxpayer data is serious, it is of some concern to the Committee that the current definition of fraud against the Commonwealth does not provide for subcategories which would clarify the nature of the reported fraud.

Recommendation 1

2.26 **The Committee recommends that the ANAO, in its preparation of a better practice guide on fraud control, develop subcategories of fraud for the purposes of fraud reporting, and discuss this issue with the Joint Committee of Public Accounts and Audit prior to finalisation of the better practice guide.**

Fraud control framework

2.27 The audit report stated that the ATO has established a comprehensive fraud control policy framework. The report noted that the ATO has also recognised the importance of an ethical and

16 Preston, *Transcript*, 2 May 2001, pp. 5-6.

17 *Transcript*, 2 May 2001, p. 6.

18 *Transcript*, 2 May 2001, p. 6.

well controlled environment in maintaining community confidence in the taxation system and, particularly, in its revenue collection responsibilities.

2.28 At the hearing, the ATO drew attention to its fraud control plan and its development of fraud and ethics training programs. The ATO explained that the training programs had been well received in terms of improving both staff understanding and the level of staff reporting of suspected fraud:

> …the ATO's internal fraud control arrangements have not stood still since the [audit] report was tabled last November. The fraud and ethics training has continued in the current financial year. To 20 April, 3850 staff have attended the first program and 2094 the second. Work has commenced on developing the third in this series of fraud and ethics training programs.
>
> Our recently established Integrity Advisory Committee has been meeting quarterly to consider issues bearing on sustaining and reinforcing an integrity based ATO. A major focus has been the establishment of an integrity adviser position for the ATO. The integrity adviser would advise ATO officers and the ATO more generally on ethics and integrity issues that can arise in interactions with taxpayers, service providers to the ATO, and in normal administration. …we expect to fill the position shortly.[19]

2.29 The Committee noted the steadily increasing number of incidents of alleged fraud.[20] The level of alleged fraud reported in the ATO has steadily increased from 255 cases in 1994–95 to 373 cases in 1999–2000.

2.30 The ATO considers that the increased incidence is due to a significant improvement in staff awareness of fraud and ethics, increased staff confidence that a reported matter will receive attention and that the interests and well being of staff who report wrongdoing by other staff will be protected.[21]

---

19 Preston, *Transcript*, 2 May 2001, p. 3.

20 *Transcript*, 2 May 2001, p. 4.

21 ANAO, Audit Report No. 16, 2000-2001, p. 36.

Committee comments

2.31 The audit report identified in the ATO areas of better practice in fraud control planning, and staff education and training. The Committee considers that the ATO is moving positively in these areas.

Private binding rulings

2.32 The Committee asked about the level of fraud control assurance in relation to private binding rulings.[22]

2.33 In response, the ATO stated that the processes for issuing both public and private rulings were treated exactly the same as other processes operating inside the ATO:

> They fall clearly within the ambit of the fraud control plan for the whole ATO. They were reviewed as part of that process when the latest fraud control plan was developed.[23]

2.34 The ATO noted that the Sherman report and various ATO initiatives will require the fraud control arrangements to be reviewed again:

> The Tax Office is now going through a very protracted process of reviewing the entire private ruling process. It is looking at it end to end, rather than simply as a series of functions located in each of the tax lines, and bringing together very active management reformulated IT systems to support it and overall management of the function in our Office of the Chief Tax Counsel. …We are also creating a publicly accessible database as a result of the Sherman recommendation.[24]

2.35 In a submission to the Committee, the ATO advised that major improvements had been made by the ATO in the way it provided private binding rulings. The improvements included:

22 *Transcript*, 2 May 2001, p. 11.

23 R Mulligan, *Transcript*, 2 May 2001, p. 11.

24 Mulligan, *Transcript*, 2 May 2001, p. 12.

- new guidelines on the types of written binding advice which may be issued by the ATO and the officers who may approve such advice;
- a process to publish edited versions of the written binding advice given (with identifying features removed);
- an integrated case management system;
- the introduction of a registration number which can be used to track the progress of all requests for private binding rulings; and
- an improved process for assuring the capability of staff preparing or approving written binding advice.[25]

Committee comment

2.36 The Committee notes the measures implemented by the ATO in relation to the provision of private binding rulings. It also notes the recently released ANAO audit report on private rulings which found significant deficiencies associated with the private rulings system.[26]

Fraud prevention

2.37 ATO Business Lines are responsible for ensuring that ATO financial, administrative and management systems and processes are adequately protected from fraudulent activity.

2.38 The ATO's Financial Services Section is responsible for the preparation of the ATO's financial statements and the provision of other financial services to ATO Business Lines. This includes the review and maintenance of ATO system controls relating to the efficacy of ATO financial management.[27]

2.39 The ATO's Financial Services Section utilises a 'Certificate of Compliance' process to provide assurance that new financial

25 ATO, Submission no. 4, pp. 1-2.

26 ANAO, Audit Report No. 3, 2001-2002, *The Australian Taxation Office's Administration of Taxation Rulings*, Commonwealth of Australia, 17 July 2001.

27 ANAO, Audit Report No. 16, 2000-2001, p. 70.

systems have controls in place to prevent and detect fraudulent activity.[28]

2.40 The ANAO report noted that the Certificate of Compliance process was limited to financial systems. The ANAO considered that fraudulent activity could occur in both financial and non-financial systems and recommended that the ATO extend its 'Certificate of Compliance' process to non-financial systems.[29]

2.41 The Committee asked the ATO about ATO systems which had not been issued with certificates of compliance.[30]

2.42 In response, the ATO stated that it had been progressively examining all its financial systems and giving them certificates of compliance to ensure that the risks were being identified and appropriately managed.[31]

2.43 The Committee asked whether all systems would be subjected to certificate of compliance tests and what the time frame for the process would be.[32]

2.44 In its submission, the ATO replied that:

- certificates of compliance had been issued for all financial systems;
- when some of the financial systems were eventually decommissioned, they would become legacy[33] systems and fresh risk evaluations would need to be undertaken; and
- the ATO was yet to settle timeframes for issuing certificates for non-financial systems.[34]

Committee comment

2.45 The Committee agrees with the ANAO that there should be a certificate of compliance process for non-financial systems and expects the ATO's agreement to the ANAO's recommendation no. 5 to result in appropriate and timely implementation of such a process.

28 ANAO, Audit Report No. 16, 2000-2001, p. 70.
29 ANAO, Audit Report No. 16, 2000-2001, p. 71.
30 *Transcript*, 2 May 2001, p. 10.
31 Mulligan, *Transcript*, 2 May 2001, pp. 10-11.
32 *Transcript*, 2 May 2001, p. 11.
33 Systems no longer required because of tax reform or legislative change.
34 ATO, Submission no. 5, pp. 3-4.

IT security

2.46 Over the last two decades, both the public and private sectors have become increasingly reliant on IT systems for the performance of their core business functions. Although there are significant efficiencies generated through IT systems in areas such as data processing, data collection, and communications, protection of the information contained in these IT systems has become increasingly difficult.[35]

2.47 The ATO is reliant on its IT systems for recording information and for supporting its revenue collection systems. The ATO network can be broadly categorised into two main areas: the mainframe environment and the Wide Area Network (WAN) environment.

2.48 ATO IT Services is responsible for controlling and maintaining the data contained on the ATO mainframe, as well as user access to mainframe data. A private sector contractor is responsible for providing and supplying administrative services and platforms for the ATO mainframe environment.

2.49 The WAN environment comprises a number of linked local area network (LANs) and uses the Microsoft Windows NT operating system. A private sector contractor provides the administrative services and platform to support the WAN, including software and hardware.[36]

Outsourcing risks

2.50 The ANAO has noted in previous audits since 1994-95 that there are significant risks associated with ensuring the security of the ATO IT systems. These risks related primarily to the storage of taxpayer data on the ATO Wide Area Network and the granting and monitoring of staff access to the ATO IT systems.[37]

2.51 During the current audit, the ANAO found that not only do these risks remain, but the risk factors have increased due to the outsourcing of many IT system functions. The ANAO considers that this is due to ATO contractor staff having limited exposure to

35 ANAO, Audit Report No. 16, 2000-2001, p. 74.
36 ANAO, Audit Report No. 16, 2000-2001, p. 76.
37 ANAO, Audit Report No. 16, 2000-2001, p. 20.

ATO fraud prevention, education and awareness material and programs in comparison to ATO employees.

2.52 In addition, the ATO could not provide evidence to the ANAO that the IT Security Section had monitored outsourced contractors' activity to ensure compliance with taxpayer data security provisions of its IT outsourcing contracts.[38]

2.53 The Committee asked the ATO where taxpayer data resided within Electronic Data Systems (EDS), the outsourced service provider.[39]

2.54 The ATO replied that the data sat in the EDS Burwood centre in Sydney on a mainframe, access to which was specifically for ATO use:

> We access it, and our ATO systems use the data from that particular location in the country. The contract as it stands does not allow that data to leave Australia.[40]

2.55 The Committee inquired whether EDS staff performing work associated with taxpayer data worked exclusively on the ATO contract, or worked on a number of contracts.[41]

2.56 In response, the ATO stated that while the majority would work specifically to the ATO, there would be a range of people brought in to address particular issues who may move on to other work.[42]

2.57 The Committee sought advice from the ATO on the measures it was implementing to address the ATO's concerns that the integrity of the data and the risk of misuse had been increased as a result of the outsourcing of the IT function.[43]

2.58 The ATO replied that it had looked again at all its vetting processes and procedures for contractors and agreed that it needed to implement more monitoring elements. It also agreed that it needed to provide evidence of monitoring.[44]

---

38 ANAO, Audit Report No. 16, 2000-2001, p. 20.

39 *Transcript*, 2 May 2001, p. 6.

40 J Growder, *Transcript*, 2 May 2001, p. 7.

41 *Transcript*, 2 May 2001, p. 7.

42 Growder, *Transcript*, 2 May 2001, p. 7.

43 *Transcript*, 2 May 2001, p. 7.

44 Growder, *Transcript*, 2 May 2001, pp.7- 8.

2.59 In response to a request by the Committee for comment on whether the risk had been alleviated by the measures being taken by the ATO, the ANAO stated:

> In this particular area, our report said that it was important that the ATO contractor staff have the same sort of exposure to the education and awareness material as the ATO runs for its own staff, so that they equally are aware of the importance and are conscious of security matters. We felt a little more had to be done there. Similarly, in the monitoring of contractor performance, we said that the ATO should focus on that as much as they focus on their own staff … We felt that the tax office needed to do a little more to recognise that the risks had changed and that there may be a need to be conscious, when they run these programs or do this monitoring for their own staff, that the contractors are included within that umbrella.[45]

2.60 The ANAO stressed that while some initial comfort might be taken from the fact that a substantial proportion of EDS staff were ex-ATO staff, it was not advisable to rely totally on that fact:

> The regime you put in place on the appointment of the outsourcer should obviously take account of the different risk profile.[46]

Committee comments

2.61 The Committee considers that when work is contracted out by an agency, the contractors' staff should be put through the same security checks as the agency's own staff and should have the same level of fraud awareness.

2.62 The Committee considers that the ATO must actively manage the risks of change, and should now have a higher awareness of what those risks are. As operations are streamlined and fewer staff are applied to a range of tasks, there is a need to understand what is happening to the risk and whether there is a need to compensate in any way.

45 I McPhee, *Transcript*, 2 May 2001, p. 9.

46 McPhee, *Transcript*, 2 May 2001, p. 9.

Firecall

2.63 To facilitate the smooth operation of ATO IT systems it is necessary at times for ATO IT systems staff to make direct changes to ATO's mainframe environment to correct system errors. To enable staff to perform these quick fixes and to gain the necessary direct access to production data in the mainframe environment, the ATO has a special access authority known as *Firecall* to bypass security controls.[47]

2.64 The ANAO first raised concerns about the use of *Firecall* in 1994-95 and noted that, many ATO staff were not only using *Firecall* for emergency situations, but also to perform their normal daily work. Since then the ANAO has noted that *Firecall* continues to be used so frequently that effective, independent review by the ATO IT Security Section is administratively unachievable.[48]

2.65 The ATO advised the ANAO that it was in the process of introducing systems changes and revising its policies to restrict the use of *Firecall*.[49]

2.66 The ANAO's audit report gave details of ATO *Firecall* usage to August 2000. The Committee asked whether there had been any peaks is the use of *Firecall* since June 1999.[50]

2.67 The ATO reported that in recent discussions with the ATO, it had been suggested that there had been a peak at the beginning of 2001, and the ATO was investigating that issue.[51]

2.68 The Committee asked the ATO whether, on an ongoing basis, it planned to sample *Firecall* usage or review each use of *Firecall*.[52]

2.69 In reply, the ATO stated:

> We want to get to 100 per cent. We do have the data for 100 per cent. We are logging all accesses to Firecall, but we want to get to the point where we can look at each one of those to be totally satisfied in that regard.[53]

47 ANAO, Audit Report No. 16, 2000-2001, p. 21.
48 ANAO, Audit Report No. 16, 2000-2001, p. 21.
49 ANAO, Audit Report No. 16, 2000-2001, p. 21.
50 *Transcript*, 2 May 2001, p. 12.
51 Growder, *Transcript*, 2 May 2001, p. 12.
52 *Transcript*, 2 May 2001, p. 13.
53 Growder, *Transcript*, 2 May 2001, p. 13.

2.70 The ATO confirmed that when *Firecall* access was used to keep the system running , it was generally EDS usage. There were particular instances when ATO staff used *Firecall*:

> Essentially, what we are talking about in the instances of ATO staff using Firecall are instances where production application systems have failed, aborted or broken down for whatever reason, mostly due to corrupt data, and Firecall is used with appropriate authorisation to remove the corrupt data and re-establish the production processing.[54]

Committee comments

2.71 The ANAO report noted that *Firecall* alter and update usage between December 1999 and January 2000 was 24 911. The ATO stated that this dramatic increase in *Firecall* usage in December 1999 and January 2000 was due to significant changes made to ATO IT systems as part of its tax reform program and these changes required the use of *Firecall*. The ATO has acknowledged that inappropriate use of the *Firecall* facility has also been a contributing factor.[55] The ATO advised the Committee that expected use of *Firecall* would normally be in the range of 200 to 300 per month.[56]

2.72 The Committee understands that *Firecall* is a facility that provides a mechanism to bypass all security controls and provides a user with unrestricted access to everything on the mainframe computer.

2.73 While there are appropriate controls on *Firecall*, and uses are logged and have the capability to be monitored, the Committee considers that the reasons for the high levels of usage need to be addressed. It is not possible for high levels of usage to be actively monitored.

2.74 The Committee notes that the ATO is in the process of introducing systems' changes and revising its policies to restrict the use of *Firecall*.

54 W Collins, *Transcript*, 2 May 2001, p. 14.

55 ANAO, Audit Report No. 16, 2000-2001, pp. 86–87.

56 M Hirschfeld, *Transcript*, 2 May 2001, p. 13.

2.75 The ATO should ensure that if staff or contractors currently using *Firecall* for certain purposes are provided with an alternative mode of access, the alternative access has adequate controls and is able to be properly monitored.

3

Audit Report No. 22, 2000-2001

Fraud Control in Defence

Department of Defence

Introduction

3.1 Fraud detection, prevention and control are important in maintaining public confidence in the ability of government departments to exercise adequate control over the expenditure of public resources.

3.2 There are many definitions of fraud. The ANAO defined fraud as 'obtaining money or other advantages by dishonest means.'[1] However, fraud is not restricted to money or material benefits. It can include 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]

3.3 The Attorney-General's Department released a consultation draft on Commonwealth fraud control policy and guidelines in April 2001. The draft described fraud against the Commonwealth as 'dishonestly obtaining a benefit by deception or other means'.[3] This definition includes:

---

1 ANAO, Report No. 22, *Fraud Control in Defence*, 2000-2001, Commonwealth of Australia, 14 December 2000, p. 11.

2 ANAO, Report No. 22, 2000-2001, p. 11.

3 Attorney-General's Department, *Commonwealth Fraud Control Policy and Guidelines– Consultation Draft No 2*, April 2001, p. 4.

- theft;
- obtaining property, a financial advantage or any other benefit by deception;
- causing a loss, avoiding or creating a liability by deception;
- providing false or misleading information, or failing to provide information where there is an obligation to do so;
- making, using or possessing forged or falsified documents;
- bribery, corruption or abuse of office;
- unlawful use of Commonwealth computers, vehicles, telephones and other property or services;
- bankruptcy offences; and
- committing any offences of a like nature to those listed above.[4]

3.4 The nature of fraud often makes it difficult to detect. There have been several attempts to quantify the value of fraud committed in Australia. The Australian Institute of Criminology has estimated that fraud in the public and private sector 'costs the community between $3 billion and $3.5 billion per year. This makes fraud the most expensive category of crime in Australia.'[5]

3.5 Defence expenditure amounts to $13 billion per year and it has assets valued at $41 billion under its control. At the time of the audit, Defence was organised into twelve Groups: Defence Headquarters, Army, Navy, Airforce, Intelligence, Support Command, Defence Personnel Executives, Acquisition, Science and Technology, Defence Information Systems, Defence Estate, and Defence Corporate Support.[6]

3.6 The amount of fraud detected in Defence in 1999-2000 was $2.5 million. The highest level of fraud detected in Defence was in 1997-98 when determined losses amounted to $3 million.[7] The Committee was also informed about a case involving an employee defrauding Defence of nearly $200 000 in 1998–1999.[8]

---

4 Attorney-General's Department, *Fraud Control Policy and Guidelines*, pp. 4–5.

5 ANAO, Report No. 22, 2000-2001, p. 11.

6 ANAO, Report No. 22, 2000-2001, p. 22.

7 ANAO, Report No. 22, 2000-2001, p. 39.

8 Defence, Submission no. 6, p. 1; Neumann, *Transcript*, 2 May 2001, p. 26.

ANAO audit objectives and findings

3.7 The objective of the ANAO performance audit, which cost $174 000, was to establish whether Defence had 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'.[9]

3.8 In its report No. 22, 2000-2001, *Fraud Control in Defence*, ANAO found that there was scope for improvement in Defence's corporate governance surrounding fraud control. Defence's *Chief Executive Instructions* (CEIs) did not comply with the Commonwealth fraud control policy requirement to review its fraud control arrangements every two years. Furthermore, the Defence Audit Committee did not monitor Group and Sub-Group fraud control plans in accordance with CEIs.[10]

3.9 The audit found that Defence lacked a suitable fraud intelligence capability. The ANAO maintained that having a sound fraud intelligence capacity would help in assessing whether Defence had under-estimated the extent of fraud in or against Defence.[11]

3.10 At the time of the audit, two of the twelve Defence Groups did not have a fraud control plan and only 47 out of 89 Sub-Groups had approved fraud control plans. Of the fraud control plans that were completed, the ANAO found that the 'vast majority of performance indicators in the fraud control plans do not allow for regular assessment of their achievement'.[12] Furthermore, most of the development of the fraud control plans was based on risk assessment plans that were up to four years old.[13]

3.11 The audit reviewed various aspects of the operation of the Directorate of Fraud Control Policy and Ethics. The ANAO report stated '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'.[14]

9 ANAO, Report No. 22, 2000-2001, p.23.
10 ANAO, Report No. 22, 2000-2001, p.29.
11 ANAO, Report No. 22, 2000-2001, p.13.
12 ANAO, Report No. 22, 2000-2001, pp.50, 51.
13 ANAO, Report No. 22, 2000-2001, p.13.
14 ANAO, Report No. 22, 2000-2001, p.54.

3.12 The audit also examined Defence's fraud investigation arrangements. There are four separate areas in Defence undertaking fraud investigations, one from the Inspector-General division and three from the military police. The ANAO found that each area used a separate set of investigation guidelines. Furthermore, none of the military police, who investigate approximately 85 per cent of fraud cases, had obtained a *Certificate IV, Fraud Control (Investigations).* The certificate is considered the minimum industry qualification.[15]

3.13 The ANAO made six recommendations aimed at improving fraud control in Defence. Defence agreed with five recommendations but disagreed with one regarding the development of a fraud intelligence capacity. Defence stated that the 'cost of establishing an intelligence capacity would…not seem to represent good value-for-money'.[16]

Committee Objectives

3.14 The Committee reviewed the effectiveness of Defence's fraud control arrangements. A public hearing was held on 2 May 2001 when the Committee inquired into:

- Detected fraud
  - ⇒ international comparisons
  - ⇒ fraud intelligence capacity
  - ⇒ analytical techniques
- Fraud control
  - ⇒ asset register
  - ⇒ risk management
  - ⇒ financial and administrative systems
- Role of the Defence Audit Committee

15 ANAO, Report No. 22, 2000-2001, pp.56–57.

16 ANAO, Report No. 22, 2000-2001, p.41.

Detected Fraud

3.15 The amount of fraud detected in Defence during the 1999–2000 financial year was 'quite clearly a floor; it is not a ceiling'.[17] Defence explained to the Committee how the figure was determined:

> The $2.5 million figure is aggregated by taking the value of those cases that go to court and the amount that is mentioned in court or in a Defence Force magistrate hearing. We have had instances where we look at a case which might involve $4,000, or $12,000. We go to the DPP and they say, 'We feel very comfortable with that, approving it for $10,000, but not for the additional $2,000.' We would then use that $10,000 figure, and that is the figure which we would use towards that total of $2.5 million. Where it does not go to court, we are reliant upon the best estimation of the investigator who has undertaken the case.[18]

3.16 The best estimation of the investigator who has undertaken the case could arise from an audit or from other computer techniques, depending on the nature of the fraud.[19]

> Even using computer aided audit techniques, it only pulls out the ones that appear suspect for some reason. It does not pull out the ones that may have been done elsewhere, under a different name, for example, or ones where the data does not appear to be suspect, or in fact have been approved.[20]

3.17 In answer to a question taken on notice, Defence estimated that about 30 per cent of the cases comprising the $2.5 million loss were either civil court or *Defence Force Disciplinary Act* cases. In terms of monetary value, these cases represented approximately 45 per cent of $2.5 million.[21]

3.18 The Committee sought to determine whether the amount of detected fraud was a realistic indicator of the true level of fraud

---

17 C Neumann, *Transcript*, 2 May 2001, p. 27.
18 M Taylor, Transcript, 2 May 2001, p.27.
19 Neumann, Transcript, 2 May 2001, p.27.
20 Neumann, *Transcript*, 2 May 2001, p. 27.
21 Defence, Submission no. 6, p. 1.

given that Defence receives appropriations of approximately $13 billion per year and manages assets worth $41 billion. In its response, Defence referred to a 1993 UK National Audit Office report which stated it was impossible to determine whether the number of fraud cases discovered represented the majority of the frauds being perpetrated or whether the cases discovered were just the tip of the iceberg.[22] Defence also stated that 'the odd academic has also asked the same question and come to the same conclusion.'[23]

3.19 Defence explained that detected fraud is only the minimum amount of fraud that occurs.

> In all cases when you are dealing with fraud the bottom line, or the floor, is the detected amount. It is the same case with the police: the crime statistics are only the reported amount. The question in my mind really is whether there is a gap between what I call the floor and the ceiling.[24]

3.20 Defence maintained that the difference between the detected and the actual level of fraud is close. Defence noted that the amount of fraud detected has been fairly consistent over the past five years:

> …we have detected about the same amount within a fairly narrow band range. I would have expected by now that, if we were not detecting all that much, we would have had quite wild fluctuations.[25]

International Comparisons

3.21 ANAO made some international comparisons between Defence, US Department of Defence (DOD) and the Ministry of Defence in the UK. It cited a report from the US General Accounting Office on DOD, listing the following as potential fraud areas in the USA:

- Wasted resources
  - ⇒ between 1996–1998, the US Navy reportedly wrote off as lost over $3 billion in in-transit inventory;

22 Neumann, Transcript, 2 May 2001, p.19.
23 Neumann, Transcript, 2 May 2001, p.19.
24 Neumann, Transcript, 2 May 2001, p.19.
25 Neumann, Transcript, 2 May 2001, p.19.

- ⇒ In October 1997, 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; and
- ⇒ In August 1998, DOD inadvertently sold surplus parts with military technology intact.

- Serious internal control weaknesses in the US Forces, resulting in:
  - ⇒ Two embezzled Air Force vendor payments involving nearly $1 million;
  - ⇒ erroneous, fraudulent, and improper payments to its contractors;
  - ⇒ higher prices than necessary for commercial spare parts; and
  - ⇒ fraud and improper payments. [26]

3.22 The US General Accounting Office recommended that DOD upgrade the skills of its financial personnel and successfully overcome serious design flaws in its financial systems. It concluded that DOD contract management 'remains on our list of high-risk areas.'[27]

3.23 ANAO also cited a UK National Audit Office report on fraud risk in the Ministry of Defence property management which reported the 'total estimated fraud loss of those cases under investigation by the Ministry's Police Fraud Squad was £17 million'.[28] The risk areas were computer systems, non-competitive pricing, small value non-competitive contracts, local purchase arrangements, and control of assets held by contractors.[29] If this level of fraud were replicated in the Australian context, it would be equivalent to $15.2 million in cases under investigation in just the Defence Estate Organisation.[30]

3.24 While acknowledging that comparisons are problematic because of differences in both countries, nevertheless, ANAO concluded that: 'On the face of it, the comparison with the UK indicates that detected fraud may not represent the extent of actual fraud in Defence'.[31]

---

26 ANAO, Report No. 22, 2000-2001, pp.65–66.
27 ANAO, Report No. 22, 2000-2001, p.65.
28 ANAO, Report No. 22, 2000-2001, p.38.
29 ANAO, Report No. 22, 2000-2001, p.36.
30 ANAO, Report No. 22, 2000-2001, p.38.
31 ANAO, Report No. 22, 2000-2001, p.39.

3.25 At the public hearing, Defence responded from a different perspective. Given that the fraud loss of £17 million in property management cases represented 75 per cent value of frauds investigated by the UK Ministry, 'that would give you a figure of approximately £23 million worth of investigated fraud'.

> If you then go back to the end of paragraph 3.13 [of Audit Report no.22] for the total defence budget of £23 billion, that gives you a fraud level of approximately 0.1 per cent, which gives you quite a different impression from the way it has been interpreted there.[32]

3.26 Defence then cited a small worldwide organisation which had made an estimate:

> …that about 0.1 per cent of whatever population you are looking at for statistics could be characterised as fraud, including theft. So, to the extent that we have got any figure, the figure of about 0.1 seems to be about right, but with all the caveats about international comparisons, different time zones and different definitions of fraud…[33]

3.27 The Committee noted that if this 0.1 per cent benchmark was applied to the total Defence appropriation for 1999–2000, the estimated level of fraud in Defence should be $18.5 million, of which ANAO had estimated $15.2 million would apply to Defence Estate Organisation alone.[34] Asked to comment, ANAO replied:

> The reference to the $15 million … was not meant to suggest there is that totality of fraud in Defence here. It was simply meant to be a prompt to Defence here to do the kind of benchmarking we have been talking about, and it was leading up to our recommendation that there be a fraud intelligence capacity. It must be seen too in the context of our discussion of the Defence environment. Defence does not have good financial systems.[35]

32 Neumann, Transcript, 2 May 2001, p.23.

33 Neumann, Transcript, 2 May 2001, p.23.

34 Defence, *Annual Report 1999–2000*, Commonwealth of Australia 2000, p.20; ANAO, Report No. 22, 2000-2001, p.38.

35 A Minchin, Transcript, 2 May 2001, p.32.

Committee comments

3.28 Although the Committee accepts that the amount of fraud detected has been fairly consistent over the past five years in Defence, the Committee questions whether Defence has been as diligent as it could be in detecting fraud, given that its asset register 'is not in good shape'[36] and fraud investigation is undertaken in four separate areas—Inspector-General division and the military police in each of the services. In each area, a different set of investigation guidelines is used.[37] ANAO found that 85 per cent of all fraud are investigated by military police.[38] ANAO commented that among the military:

> 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.[39]

3.29 Furthermore, while staff in the Defence Directorate of Fraud Investigations and Recovery have or are seeking Certificate IV qualifications in fraud investigation, the same does not apply to the military police. ANAO recommended that competency standards for fraud detection should be set for military police engaged in fraud detection.[40]

3.30 The Committee believes that it is important that a comprehensive set of fraud investigation procedures should be developed to provide direction to fraud investigation staff. This would ensure compliance with legislative and other requirements and enhance effectiveness and efficiency in fraud investigation. Such procedural guidelines could be based on *Commonwealth Fraud Control Policy and Guidelines* issued by the Attorney-General. The Committee therefore endorses ANAO's recommendation 6, that Defence:

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

---

36 Neumann, *Transcript*, 2 May 2001, p. 21.
37 ANAO, Report No. 22, 2000-2001, p.55.
38 ANAO, Report No. 22, 2000-2001, p.28.
39 ANAO, Report No. 22, 2000-2001, p.33.
40 ANAO, Report No. 22, 2000-2001, p.57.

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

3.31 Defence agreed with this recommendation but as yet, it had not been implemented.

Fraud intelligence capacity

3.32 The Committee is aware that ANAO recommended in 1991 that Defence develop analytical techniques and audit tests to detect fraudulent transactions. ANAO found that its 2000 audit showed that Defence had not implemented this recommendation. 'Defence does not have a fraud intelligence capacity.'[41]

3.33 Defence's reluctance to develop a fraud intelligence capacity, according to ANAO, 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'.[42]

> 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.[43]

3.34 ANAO assured the Committee that development and maintenance of a credible capacity need not be resource-intensive. ANAO said it was not suggesting that Defence set up a Fraud Prevention and Control Section, as the Australian Tax Office has, but 'we are suggesting some more strategic capacity within the department to have regard to fraud, given the environment that is facing the department'.[44] ANAO reiterated that 'there is value in Defence seriously considering a greater intelligence capacity'.[45]

Analytical techniques

3.35 Defence disagreed with ANAO's recommendation because:

41 ANAO, Report No. 22, 2000-2001, p.40.
42 Underlining in original text. ANAO, Report No. 22, 2000-2001, p.40.
43 ANAO, Report No. 22, 2000-2001, p.40.
44 I McPhee, Transcript, 2 May 2001, p.32.
45 McPhee, Transcript, 2 May 2001, p.32.

> …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.[46]

3.36 At the public hearing, the Inspector-General stated it was improving its fraud control. The *Chief Executive Instructions* were amended to review fraud control arrangements every two years from July 2001. Advice on fraud related matters to assist in fraud risk assessments had been sought in March 2001 and fraud control plans based on these assessments were to be implemented in July 2001.[47] Subsequently, Defence provided to the Committee its input to the Commonwealth annual fraud control report, compiled by the Attorney-General's Department.[48]

3.37 Defence now has a full-time team of three who use computer aided audit techniques on a daily basis.

> They look for what we were talking about with respect to inefficiency and ineffectiveness as well as fraud, as well as abuse, if you like. Some of the things we use it for are debtor management, fringe benefits tax, leave processing, travel payments, which is one of our high areas, and determining the extent of fraud….[49]

3.38 When a potential fraud case is discovered, Defence tracks all the records back to try to determine the monetary amount involved. It then makes an estimate for court action purposes and court action is initiated to seek restitution.[50]

3.39 Defence also explained that staff have attended data mining courses to try to find useful patterns in the information presented and to analyse any changes. Recently a Canadian fraud detection expert working in the Canadian Department of National Defence had visited Australia and had given Defence staff a review of other analytical techniques such as ratio analysis as an assistance to computer aided audit techniques.[51]

---

46 ANAO, Report No.22, 2000-2001, p. 41.

47 Neumann, Transcript, 2 May 2001, p.30.

48 Defence, Submission no. 8.

49 Neumann, Transcript, 2 May 2001, p.31.

50 Neumann, Transcript, 2 May 2001, p.31.

51 Neumann, Transcript, 2 May 2001, p.31.

Committee comment

3.40 The Committee accepts that Defence has started developing a range of analytical techniques used to detect fraudulent activity. Nevertheless, the Committee believes there is merit in Defence developing a fraud intelligence capacity along the lines suggested by ANAO in its report since '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'.[52]

3.41 The Committee agrees with ANAO that a fraud intelligence capacity would significantly support fraud risk assessment and enhance fraud prevention and detection. Furthermore, it would provide greater assurance at reasonable cost to all stakeholders. The Committee therefore urges Defence management to benchmark its fraud prevention / detection strategies and initiatives to see if they are sufficient for the task, given Defence's wide-ranging exposures, its poor asset management records and its need to change the culture among so many Groups.

Fraud Control

3.42 The Committee sought to determine whether the controls Defence has in place were robust and sufficient to detect fraudulent activity. At the public hearing, Defence explained that although its current fraud controls to monitor assets were weak in parts, it had to weigh value for money.

> To track down toilet paper or pens is not value for money. When we get into higher value items we are looking at techniques to track them—so that automatic alarms would be set off with higher value items—but that again has a cost; it has to be monitored.[53]

3.43 The difficulties arise out in the field.

> …with equipment it is 360 degrees, so you can go anywhere with it essentially. It is only by recording assets and making supervisors track them—by electronic,

52 ANAO, Report No.22, 2000-2001, p. 41.

53 Neumann, Transcript, 2 May 2001, p.21.

> paper or whatever means—that we get controls. And we do have a strong audit program.[54]

3.44 Defence did concede that some items are tracked in bulk only, while small items such as pens and paper are not tracked at all. Firearms, however, are tracked even though the risk of their loss is greater.[55]

3.45 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. Information is disseminated by the Inspector-General Division through a newsletter that contains fraud case studies and a website accessible by 85 per cent of Defence personnel.

3.46 Group Coordinators told ANAO that they were aware of these resources. They considered 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, however, by the difficulties in obtaining uniform Defence-wide statistical information on fraud.[56]

Asset Register

3.47 Asset registers are an important part of an organisation's overall management of resources. A complete and serviceable asset register is needed if departments are to fulfil their obligations under the *Financial Management and Accountability Act* to manage resources effectively and efficiently. Accurate and up-to-date asset registers are essential in a fraud control context.

> If a thing has been recorded, we can probably tell you whether we have still got it. If the thing has never been recorded, there may be no record that we ever had it. In that case, have we actually lost it? How can we prove to you that we have actually lost it? That is the question.[57]

3.48 Defence admitted that its 'asset register is not in good shape'. The Inspector-General explained:

54 Neumann, Transcript, 2 May 2001, p.21.
55 Neumann, Transcript, 2 May 2001, p.23.
56 ANAO, Report No.22, 2000-2001, p. 44.
57 Neumann, Transcript, 2 May 2001, p. 21.

> …we are still moving from the historical to what we regard as good management practice. There is no doubt about that. So we are still on that curve. The very fact that for the last three fiscal years we have had quite large amounts of assets first found shows that the asset registers are not complete.[58]

3.49 Defence acknowledged that it needed accurate registers for two reasons: good management and proof of legal ownership. Its asset register posed a real challenge as Defence moved from cash accounting to an accrual basis. Part of the problem in Defence is that purchases occur in many different scattered areas. There needs to be efficient entry of such purchases into the asset register because 'if they are not put on the register…when they are bought, they are not recorded'.[59]

> Therefore, even if, at the end of the day, the investigators come around, for whatever reason, and say, 'We think the person's actually stolen this,' to prove it is going to be almost impossible in a court of law. [60]

3.50 Defence told the Committee that the Chief Financial Officer has committed to getting the asset register into a serviceable shape within one year. This involved ensuring system integrity and governance so that the different charts of accounts are able to interact and interrogate each other.[61] The audit report listed several matters requiring significant improvements:

- 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

58 Neumann, Transcript, 2 May 2001, p. 24.
59 Neumann, Transcript, 2 May 2001, p. 24.
60 Neumann, Transcript, 2 May 2001, p. 24.
61 Neumann, Transcript, 2 May 2001, pp.24–25.

⇒ key asset management data is not collected. The costs of maintaining assets are an important element of informed replace / retain decisions.[62]

3.51 Questioned about this estimated understatement of assets, totally $350 million, the Inspector-General appeared unsure, since the value was notional only although he believes 'these are actually parts'. He explained some of the difficulties in cataloguing asset items such as an aircraft engine. 'Is it still part of the aircraft and recorded as part of the aircraft, or is it recorded as a part of the spares system?'[63]

> Basic issues like that were worked out—and are still being worked out, I think, in some of the inventory systems—because, when you have a cash budgeting system, you do not actually account, measure, or whatever all your inventory. And the thing about accruals is that you have got to count everything, starting from the land upwards and across-way…[64]

Committee comment

3.52 The Committee found this system somewhat bizarre since fraud would be very hard to detect if Defence's various asset systems are not compatible, are incomplete and values of some assets are not known. The Inspector-General agreed: 'if the thing is not recorded on the system or is misrecorded on the system, you will never know'.[65] Given these inexactitudes, the Committee found it puzzling that Defence did not do more about establishing some procedures to circumvent irregularities, potential fraud or petty theft.

Recommendation 2

3.53 **The Joint Committee of Public Accounts and Audit recommends the Department of Defence address the shortcomings in its asset registers and report back to the Committee on the condition of its asset registers in July 2002.**

62 ANAO, Report No.22, 2000-2001, p. 34.
63 Neumann, Transcript, 2 May 2001, p. 33.
64 Neumann, Transcript, 2 May 2001, p. 33.
65 Neumann, Transcript, 2 May 2001, p. 33.

Risk Management

3.54 Defence maintained that its fraud detection was based on a risk management approach. Defence stated:

> In terms of risk, you do the high value and in our case probably more dangerous things we hold in greater detail. Certainly the risk of losing a personal firearm is much higher, (1) because it is smaller to conceal, (2) it is more attractive and (3) it is easier to get away with than a bomb or a missile. But they are also tracked.[66]

3.55 Other items such as uniforms are tracked in bulk but not individually.[67] Defence concluded that their auditors are finding that the bulk of waste is from mismanagement of resources rather than fraudulent activity. When questioned on whether Defence has gone through area by area and made rational judgements about what likely losses there are and what the cost of detection is, Defence responded:

> With fraud you have to prove intent, particularly to get a conviction. In the US they use the term 'waste and abuse'.[68]

3.56 Defence explained that the UK National Audit Office made it quite clear that a lot of people will give contractors and others the benefit of the doubt.

> They regard it as sharp practice rather than automatically assuming that people are being fraudulent or thieving. Therefore, they may not report something because they think it is sharp commercial practice rather than an intent to deceive. But proving intent to deceive is actually quite difficult.[69]

3.57 The Committee believes that all fraud control plans should be based on recent fraud risk assessments to ensure that the plans reflect the current circumstances. 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 and management.

---

66 Neumann, Transcript, 2 May 2001, p. 23.

67 Neumann, Transcript, 2 May 2001, p. 23.

68 Neumann, Transcript, 2 May 2001, pp.23–24.

69 Neumann, Transcript, 2 May 2001, p. 24.

Financial and Administrative Systems

3.58 The current state of Defence financial and administrative systems has been subject to prolonged criticism by the ANAO and recognised as an area of concern by the then Minister for Defence and Secretary of the Department. The ANAO reported that the condition of the financial and administrative systems contributed to the overall levels of risk in Defence's environment.[70]

3.59 In November 2000, the then Minister for Defence listed 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.'[71]

3.60 In evidence to the Committee, Defence explained its administrative arrangements for fraud detection. It advised that 85 per cent of fraud related cases are investigated by the military police. The Inspector-General investigates the more serious cases involving $5000 or more, and / or more sensitive cases, such as those involving senior officers. Where the military police are investigating something which looks as if it may be serious or sensitive, they then consult the Inspector-General.

> …we have a discussion as to who investigates it and also under which jurisdiction we do that investigation. That generally works quite well. There will be occasions where the Inspector-General Division will get a case which is below $5,000 which we think would be more appropriately done by military police and we will refer it to them.[72]

3.61 At present, Defence is not able to provide complete information on the 85 per cent of fraud cases investigated by the military police. Once its new case management system is fully operational, however, Defence will have data on specific types of fraud. There is still fine-tuning required and data from the Army needs to be incorporated fully.[73]

---

70 Minchin, *Transcript*, 2 May 2001, p. 32; ANAO, Report No. 22, 2000-2001, p.32.

71 ANAO, Report No. 22, 2000-2001, p.35.

72 Taylor, Transcript, 2 May 2001, p. 25.

73 Taylor, Transcript, 2 May 2001, p. 25.

3.62 The Committee inquired how Defence obtains an organisational wide view of fraud in Defence given the current limitations. Defence stated:

> We make annual returns to the Attorney-General's Department which are not of this detail but which do give the picture for the whole of Defence. That will include the investigations from the service police—not broken down into this amount of detail, but certainly giving an organisational picture of what is happening.[74]

3.63 On examining a copy of Defence's annual returns to the Attorney-General's Department, the Committee found that it covered:

- Fraud control plans and risk assessments;
- Agency relationship with the AFP and DPP;
- Awareness, prevention, detection and investigations training;
- Investigations;
- Use of administrative remedies and recovery of money; and
- Agency investigators.[75]

Committee comment

3.64 The Committee noted that discussion related to each heading in Defence's annual returns to the Attorney-General's Department was general and aggregated. Its annual returns cannot be used other than to give a very broad overall picture of fraud control in Defence. The Committee is not convinced that the financial and administrative systems Defence has in place are sufficient to obtain an adequate organisational view of the occurrence of fraud in Defence.

3.65 In relation to the level of fraud control Defence has in place to safeguard public funds, the Committee notes that:

- there is scope for improvement in the asset register;
- Defence still needs to undertake a risk management exercise into what assets in what areas will need to be tracked and monitored; and

74 Taylor, Transcript, 2 May 2001, p. 26.

75 Defence, Submission no. 8.

- the inadequate state of the financial and administrative systems contributes to Defence's overall fraud risk environment.

3.66 Defence maintained that developing a fraud intelligence capability was not value for money given that 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.'[76]

3.67 The Committee is persuaded that given Defence's current fraud control arrangements and that the Inspector-General Division conceded that 'fraud control has not been accorded high priority by some Groups in Defence',[77] Defence needs to put in place better controls to ensure fraud is detected and effectively managed. Namely, Defence needs to develop a fraud intelligence capability.

Recommendation 3

3.68 **The Joint Committee of Public Accounts and Audit recommends that the Department of Defence immediately implement the Australian National Audit Office recommendation that it develop a fraud intelligence capability to ensure better management of public funds and increase its ability to detect fraudulent activity in Defence.**

Role of the Defence Audit Committee

3.69 In the Defence 1999-2000 Annual Report, there is a reference to the Defence Audit and Program Evaluation Committee (now known as the Defence Audit Committee (DAC)) addressing fraud, theft and loss of information.[78] The Committee asked Defence about the role of the DAC in this area. Defence responded that since December 2000, DAC had meet three to four times and fraud control planning has been on the agenda at each of these meetings. Prior to this, fraud may have been discussed once or twice a year.

76 ANAO, Report No. 22, 2000-2001, p.41.

77 ANAO, Report No. 22, 2000-2001, p.48.

78 Defence, *Annual Report 1999-2000,* p.63.

> …it certainly brought it into more prominence. There is also a follow-up now. The Chair of the Audit Committee now briefs the Defence Committee on issues. On the last occasion, I know he was very forthright in his comments about fraud control planning and the failure of one Group to do it on time.[79]

3.70 Another DAC role was to monitor and take action on recommendations from the ANAO, internal audit and the JCPAA. DAC will make staff report on outstanding issues regarding such recommendations.

> …[this] will focus managers' attention on the fact that they cannot just simply agree to a recommendation from either the Australian National Audit Office or management audit and then not follow through with it.[80]

3.71 DAC will call upon Defence staff to explain why the implementation of the recommendations is overdue so there is a follow-up mechanism.

> By the end of the financial year, I am hoping it will cover internal audit, Joint Committee of Public Accounts and Audit and Australian National Audit Office, both the financial and the performance audit; at the moment the financial reside in another group. The intention is to consolidate the whole lot. I wrote to the secretary recently and gave him a picture of how many outstanding ones we had.[81]

3.72 The Committee notes Defence's putting in place controls to ensure that recommendations made by the ANAO, Defence internal audit and the JCPAA are routinely monitored. The Committee expects the implementation of follow-up mechanisms to systematically report on outstanding recommendations which have not been implemented. Such reporting requirements will assist Defence in its fraud control.

---

79 Neumann, Transcript, 2 May 2001, p. 28.

80 Neumann, Transcript, 2 May 2001, p. 29.

81 Neumann, Transcript, 2 May 2001, p. 29.

4

Audit Report no.26, 2000–2001

Defence Estate Facilities Operations

Department of Defence

Introduction

Background

4.1 The Defence Estate comprises the land, buildings and other facilities that Defence uses across Australia. These facilities are vital to achieving the Defence mission—to prevent or defeat the use of armed force against Australia or its interests.[1] The Estate has a gross replacement value of $14.8 billion. Management of the Estate was dispersed across the various Groups in Defence until the Defence Estate Organisation (DEO) was created in 1997 to manage the Estate. This was done as part of the Defence Reform Program following a recommendation of the 1997 Defence Efficiency Review which suggested that an acceptable timeframe for the implementation of recommended changes was two to three years.[2]

4.2 Prior to the Defence Efficiency Review, funding for both capital works and facilities operations came from the Defence Portfolio

---

1 ANAO, Report No.26, 2000-2001, *Defence Estate Facilities Operations*, December 2000, p. 21; Department of Defence, *Defence 2000—Our Future Defence Force*, Commonwealth of Australia, October 2000.

2 ANAO, Report No.26, 2000-2001, pp. 21–22.

budget, with funding for facilities operations managed by Defence's individual Groups. Previously, responsibility for maintenance and minor new works rested with the establishment occupier/client, who had complete control of resources allocated for this task. Regional commanders were therefore able to determine maintenance and new work priorities for those facilities within their jurisdiction. As Defence explained at the public hearing: 'properties that the Army were on were Army properties and properties that the Navy were on were Navy properties'.[3] The creation of DEO required significant changes in the culture, management approach and practices associated with facilities management.[4]

4.3 Since 1997, DEO's Facilities Operations (FACOPS) Program has delivered general maintenance and minor new works to Defence facilities on a regional basis across the country. DEO's Estate Operations and Planning Branch and its nine Regional Estate Centres (RECs) are responsible for the FACOPS Program. Resources available for the Program have been reduced in recent years. The total DEO budget for 2000–01, which included funds for capital works, facilities operations and property management, was $2.6 billion. Of this total, the FACOPS Program had a cash allocation of $213m and an additional $15.6m for employee expenses associated with the Program's 283 staff.[5] In 2001–2002, DEO's allocation was $2.72 billion, of which $235m went to FACOPS and $17m was for salary and related items.[6]

Scope of audit

4.4 In Audit Report No. 26, 2000–2001, *Defence Estate Facilities Operations*, the audit objective was to assess the efficiency and effectiveness of selected Defence facilities operations, including tendering and contracting, with a view to making practical recommendations for enhancing operations. Relevant issues on facilities operations raised by Defence's Management Audit Branch (internal audit) in 1997, were addressed by ANAO in its audit.[7]

---

3 R Corey, *Transcript*, 2 May 2001, p. 51.

4 See DEO organisational diagram in ANAO, Report No.26, 2000-2001, p. 29.

5 ANAO, Report No.26, 2000-2001, p. 23.

6 Defence, Submission no. 9, p. 1.

7 ANAO, Report No.26, 2000-2001, p. 24.

4.5 The focus of the audit was on the following:

- DEO awareness of its 'clients', and client needs, given funding constraints;
- The extent client requirements and identified corporate priorities are taken into consideration;
- The tendering and management of DEO maintenance contracts in accordance with Commonwealth and Defence purchasing requirements (including Defence's *Chief Executive Instructions*);
- The extent FACOPS management information system informed decision-making; and
- How estate needs are identified so that works can be undertaken appropriately.

Audit findings

4.6 ANAO found that DEO had implemented many of the recommendations arising from the Defence Efficiency Review and had achieved savings through the reduction of duplicated services within each region and from the development and implementation of more efficient delivery methods. However, there was scope for improvement in various areas of the FACOPS program, particularly in relation to the management of contracts and resources.[8]

4.7 ANAO noted that significant staff reductions made within a relatively short timeframe had decreased the corporate memory, knowledge base and skills available to DEO. This drawback was further compounded by the introduction of new and significantly different management practices, yet there was no systematic monitoring by DEO of contract performance to check work done. Furthermore, not all DEO contract management staff had the appropriate skills to manage large, complex facilities maintenance contracts in the Defence environment.[9]

4.8 Following the creation of DEO, the emphasis was to deliver estate services on a priority basis by region rather than by individual establishment. In practice, this was not always the case, with variations in regional procedures resulting in a lack of transparency in decision making and with funding not always

8 ANAO, Report No.26, 2000-2001, p. 12.

9 ANAO, Report No.26, 2000-2001, pp. 53–55.

being applied to identified priorities.[10] Because regular two-way consultation between DEO and some clients did not occur, this impacted adversely on DEO's ability to deliver the FACOPS Program efficiently and effectively, and on associated client satisfaction.[11]

4.9 ANAO also found that maintenance of the Defence Estate was less than the property industry benchmark by about $100 million in 2000–2001, although the makeup of the industry benchmark is ill-defined. As a result, it appeared that needed maintenance was being deferred—as was observed during the audit. The longer-term consequences of deferring maintenance have significant implications for Defence operational requirements, funding requirements and legal responsibilities.[12]

4.10 DEO does have limited control processes to ensure that agreed facilities work projects are completed according to priorities identified in the bid process. Currently, funds allocated to RECs are at times spent on lower priority work without consultation with and agreement by Central Office. While accepting the need for flexibility given the scale of the Program, ANAO argued that it was important that there be clear understanding and communication between the RECs and Central Office in order to ensure effective management and oversight of the pre-determined priorities.[13]

4.11 ANAO concluded that basic procurement requirements were not being met efficiently and effectively in all cases in some RECs. Examples found included continually extending standing offers without testing the market; continuing to use contractors' services when the contractual relationship was unclear; and awarding substantial amounts of work to contractors without seeking other quotes.[14]

4.12 Some staff demonstrated only limited awareness and ability to apply appropriate procedures relating to the commitment and expenditure of public money. ANAO was concerned that in some instances, documents relating to procurement decisions and necessary to support payments, had been unavailable to the audit

10 ANAO, Report No.26, 2000-2001, p. 74.
11 ANAO, Report No.26, 2000-2001, pp. 72–77.
12 ANAO, Report No.26, 2000-2001, pp. 91–93, 94–95.
13 ANAO, Report No.26, 2000-2001, pp.71–75.
14 ANAO, Report No.26, 2000-2001, p. 46.

team. Evidence indicated that purchase orders had frequently been raised with minimal supporting documentation. There had also been instances of purchase orders for more than $1 million raised by staff without the appropriate authorisation or delegation. This was clearly contrary to Defence's *Chief Executive Instructions.*[15]

4.13 Undue emphasis on spending for the purpose of meeting expenditure targets is not in the Commonwealth's budgetary or contractual interests nor does it assist program efficiency. Yet ANAO found there was a continued focus on expenditure to achieve annual budget targets in DEO. Monthly expenditure of funds increased significantly towards the end of the financial year. In some cases there were overspends without approval. ANAO was told by the Estate Operations and Planning (EOP) Branch that over-spending was a positive outcome 'because it contributed to the overall achievement of budget targets by the Defence Portfolio'.[16]

4.14 Defence agreed with all six ANAO recommendations and advised that Defence Estate Organisation was supportive of the content of the audit and appreciated the consideration that ANAO gave to DEO's views in preparing the audit report.

4.15 The Committee examined the following issues at its public hearing on Wednesday 2 May 2001:

- Corporate governance
  - ⇒ Strategic Plan
  - ⇒ Chief Executive Instructions
- Facilities maintenance
  - ⇒ Data collection
  - ⇒ Maintenance benchmark
- Contract management
  - ⇒ Comprehensive maintenance contracts
  - ⇒ Staff training
- Financial management
  - ⇒ End of financial year spending
  - ⇒ Sale and lease back

15 ANAO, Report No.26, 2000-2001, pp. 52–53.

16 ANAO, Report No.26, 2000-2001, p. 75.

Corporate governance

4.16 The Committee was told that DEO had made a significant effort to develop and implement a strategic, corporate-focused framework for the delivery of maintenance work through its FACOPS Program. Initiatives, such as the Comprehensive Maintenance Contract (CMC), focus on economies and efficiencies that earlier approaches and/or methods lacked. The introduction of Total Estate Management (a comprehensive approach to managing estate assets) is meant to provide firm data on the condition of the Estate in order to substantiate maintenance funding bids and to help prioritise maintenance.[17] This was to replace the former practice whereby:

> The Army, the Navy and the Air Force each managed their own facilities operations and under the guidance of a central organisation, but then they had sub-budgets down to bases and many of the decisions were at the discretion of the base commander, but they were still managed within a single service environment.[18]

4.17 However, ANAO found that variations in regional procedures resulted in a lack of transparency in decision making and funding was not always being applied to identified priorities.[19] In effect, responsibility for maintenance and minor new works seemed still to rest with the establishment occupier/client.

Strategic Plan

4.18 In 1998, DEO prepared a Strategic Plan for Defence Estate as a guide for the next 20-30 years, 'justifying some of the decisions we were making in the way we were managing the estate'.[20] This Plan had been accepted by its Executive in December 1998 but had not received Government approval. When asked about this at the public hearing, Defence explained that the previous Defence Minister had wanted further consideration on several proposals.

> The Strategic Plan projects which bases have a long-term future, which ones have a medium-term future and which

17 I McPhee, *Transcript*, 2 May 2001, p. 36.
18 Corey, *Transcript*, 2 May 2001, p. 37.
19 McPhee, *Transcript*, 2 May 2001, p. 37.
20 Corey, *Transcript*, 2 May 2001, p. 37.

> ones have no future. In doing that, there were some implications that the Minister felt we needed to do some more work on before we put it to the government.[21]

4.19 This re-drafting was overtaken by the *Defence 2000* white paper, whose review of defence needs, strategic interests and objectives resulted in the DEO Strategic Plan being further revised. The amended version is to be considered by the Defence Committee in late 2001. Once it gains endorsement by the Defence Executive, the Plan will be submitted to the Minister for government consideration. Defence accepts that 'they may endorse it in principle but still want us to come forward with individual rationalisations, base closures and those sorts of things on a case by case basis.'[22]

4.20 Furthermore, since the draft Strategic Plan was developed, DEO has developed a strategic facilities appraisal model to help it manage the entire asset life-cycle within a framework of strategic planning and management guidance:

> We have a strategic facilities appraisal model which…talks about the capability contribution of the asset and grading it. There is an expectation that the ADF [Australian Defence Force] will give us input into what the capability contribution of each asset is. Then we will look at the condition of each asset, which is fairly simple for the industry to take on board, and look from that at the capability impact of not doing the work inside a restricted budget. That also has to be done in consultation with the Australian Defence Force.[23]

4.21 Defence told the Committee that it anticipates that within its current budget limits, it can identify and apply a risk management profile to potential and required repair and maintenance work, by using Australian Standard 4360 on risk management.

> We are going to migrate that across the entire estate so that we can look at occupational health and safety aspects, the risk of deterioration of the asset, and profile the risks that are being carried by the Department. In this way we believe we will be able to identify to the Executive what risks they are carrying and not just say,

21 Corey, *Transcript*, 2 May 2001, p. 58.

22 Corey, *Transcript*, 2 May 2001, p. 58.

23 Hammond, *Transcript*, 2 May 2001, p. 55.

> 'The model says two per cent of the gross replacement value is what we should spend on maintenance,' because that really does not tell us what a risk management profile would tell us.[24]

4.22 The Committee acknowledges that the de facto implementation of the draft Strategic Plan has assisted to some extent the gradual culture change needed in Defence. However, based on the evidence received, it is clear that DEO still has some way to go in achieving the desired culture change.

Chief Executive Instructions

4.23 When questioned about the extent regional staff are aware of the *Chief Executive Instructions,* Defence acknowledged that staff were 'probably not as aware as they should be'.[25] The Committee believes this is understating the situation, given ANAO found that, in the regional offices, staff were:

- Continuing to use contractors despite the contractual relationship being unclear;
- Continually extending standing offers without testing the market;
- Awarding substantial amounts of work to contractors without seeking other quotes;
  - ⇒ the total value of these contracts was $900 000 in 1999–2000;
- Mislaying current contracts and supporting documents in some RECs;
- Raising some purchase orders, with minimum support documentation or without appropriate delegation or authorisation;
- Sanctioning end-of-the-financial-year expenditure surges.[26]

4.24 DEO assured the Committee that it was endeavouring to correct this situation. Annual workshops on *Chief Executive Instructions* were conducted for senior staff, who were then expected to pass on this training to more junior staff. 'We have made a concentrated effort, particularly since the ANAO has highlighted

24 Hammond, *Transcript*, 2 May 2001, pp. 55–56.

25 Corey, *Transcript*, 2 May 2001, p. 55.

26 ANAO, Report No.26, 2000-2001, pp. 46, 48–49, 52–53, 77.

some of the deficiencies in the awareness of our staff, and we intend to continue that'.[27]

4.25 The Committee believes that a filter-down effect is insufficient to achieve cultural change, given that in 2001, ANAO found that Defence's implementation of audit recommendations from its 1999–2000 report on Defence estate project delivery 'has had little effect'[28] and during this audit, REC staff 'were not aware that an updated version of the *Chief Executive Instructions* had been issued'.[29] In order to effect a culture change, Defence has to ensure that all line officers develop the practice of consulting the *Chief Executive Instructions* before they enter into any contract or agreement to purchase goods and services.

Facilities maintenance

4.26 Defence's official property asset register is held in its accounting system, ROMAN, which records the address and a unique property ID number against each property.[30] There is a sub-level database that contains more details on actual items such as plant, air-conditioning units and other equipment. This sub-level database, introduced in 1997, is called the Defence Estate Management System—Facilities Maintenance (DEMS/FM), which assigns a bar-code to each individual equipment system associated with each building.[31] It is designed to standardise DEO's facilities maintenance software and create a comprehensive asset register of all Defence Estate property. It is managed by DEO and maintained and operated by an external contractor.

> …(DEMS/FM) has the capacity to capture cost data against individual facilities and link this information to the appropriate user Unit. To date this source of data has not been used for reporting actual expenditure by the nine Regional Estate Centres.[32]

---

27 Corey, *Transcript*, 2 May 2001, p. 55.

28 ANAO, Report No.26, 2000-2001, p. 77.

29 ANAO, Report No.26, 2000-2001, p. 77.

30 B Lane, *Transcript*, 2 May 2001, p. 57; Defence, correspondence with JCPAA, 2 May 2001.

31 Lane, *Transcript*, 2 May 2001, p. 57.

32 ANAO, Report No.26, 2000-2001, p. 30.

4.27 The Committee was told that the effectiveness of Estate management could be significantly improved if better information were available to target where scarce maintenance resources should best be spent.[33]

> This would include information on actual costs for attribution to Defence outputs and on the contribution each asset makes to Defence capability. ADF input is essential here, to ensure the estate management decisions are justified under Defence priority and cost effectiveness grounds.[34]

4.28 As Defence itself acknowledges in its draft Strategic Plan for the Defence Estate:

> While it is difficult to assess the validity of existing asset data, the trend in asset growth and in ageing is clear enough and has implications for maintenance (which tends to increase with age) and for overall estate management. Priority should be given to further development of the Defence Estate Management System (DEMS), and to the universal application of Asset appraisal—a maintenance planning process.[35]

Data collection

4.29 Funding allocation in relation to the Defence Estate is made by the Defence Portfolio, with professional property management advice from DEO and military advice from the facilities users—the capability output managers. Effective management of the Defence Estate requires accurate and relevant data. At this stage, however, DEO lacks sufficient detailed data to support such advice.[36] ANAO found evidence to show that 'DEO's financial data is never absolutely accurate, and that it is not uncommon for DEFMIS [the former system] and ROMAN to vary by several million dollars, with no way of judging which system is more accurate'.[37] This has impacted on DEO's ability to manage accurately its expenditure against pre-determined budget targets.

---

33 McPhee, *Transcript*, 2 May 2001, p. 37.

34 McPhee, *Transcript*, 2 May 2001, p. 37; ANAO, Report No.26, 2000-2001, p. 12.

35 ANAO, Report No.26, 2000-2001, p. 96.

36 ANAO, Report No.26, 2000-2001, p. 35.

37 ANAO, Report No.26, 2000-2001, p. 84.

4.30 The Committee believes that comprehensive information is crucial, if informed decisions on maintenance funding and expenditure are to be made. This is especially so now that Defence funding for maintenance and construction has been reduced.

Defence Estate Management System—Facilities Maintenance

4.31 DEMS/FM was designed to be a single, authoritative source of asset data, used in support of estate management activities at any point in the asset cycle (planning, acquisition, operation, and disposal). It is available on the internet to all its users—including contractors—with encryption access.[38] DEO uses DEMS/FM to collate and interrogate its data. DEMS/FM was introduced into the RECs to provide staff with a common application for managing their facilities activities. Central Office should be able to review data input into the system.[39]

4.32 Each financial year, FACOPS and each REC submit their asset maintenance bids via DEMS/FM in order to assist longer-term planning.[40] The Works Processing Module has been specifically designed to enable contractors to manage Work Requests and prepare invoices through DEMS/FM.[41]

4.33 DEMS/FM is linked to all DEO contracts and is used for tendering purposes because it is more comprehensive than the ROMAN data.[42] DEMS/FM, however, cannot effectively interact with ROMAN[43], although work is underway to put those links in place. 'Linking ROMAN to DEMS/FM will further enhance the system to keep the official ROMAN data up to date'.[44] Currently, the Australian Valuation Office is conducting three year rolling audits to validate the ROMAN data.[45]

4.34 Given this reliance on DEMS/FM, it becomes crucial for systematic recording of all facilities maintenance data, otherwise

38 ANAO, Report No.26, 2000-2001, pp. 80–81.

39 ANAO, Report No.26, 2000-2001, p. 80.

40 ANAO, Report No.26, 2000-2001, p 60.

41 ANAO, Report No.26, 2000-2001, p 81.

42 Defence, correspondence with JCPAA, 2 May 2001.

43 ANAO, Report No.26, 2000-2001, pp. 84–88; Defence, correspondence with JCPAA, 2 May 2001.

44 Defence, correspondence with JCPAA, 2 May 2001.

45 Defence, correspondence with JCPAA, 2 May 2001.

the regions are unable to make informed decisions when managing the Defence Estate. This could impact on their asset maintenance bids each year.

4.35 During the audit, ANAO found that there were a number of problems with DEMS/FM. There is no consistent and regular usage by REC staff, many of whom see its use to be limited to urgent and unforeseen property maintenance.[46] In addition:

- Connectivity problems exist, making the system very slow and causing frequent disconnections, as a result of the insufficient bandwidth available to some RECs and DEO out-stations.[47]
- Most REC staff have low user skills and many are unwilling to self-train.
  - ⇒ Some staff continue to use other applications to manage their facilities works.[48]
- There is a lack of consistency in terminology, descriptions and processes across the regions.
  - ⇒ Some of the Expenditure Groups and account codes under the current bid process no longer correspond with terms still in general use in the regions.[49]
- All the above make it difficult to extrapolate accurate reports from the database.

4.36 ANAO stated that the extent of inaccurate FACOPS Program data in DEMS/FM was unknown.[50] DEO was attempting to address this problem through the compulsory use of DEMS/FM and use of the terminology defined in the DEMS/FM *Documentation Manuals*.[51] A DEMS/FM Development Team had been set up to analyse user practices in the regions, assess the technical difficulties and to provide limited training.[52] The user interface will be made more user-friendly by means of another more commonly available application.[53]

4.37 Despite these difficulties, Defence informed the Committee that it is reasonably confident that its register stays up to date since 'we

46 ANAO, Report No.26, 2000-2001, p. 81.
47 ANAO, Report No.26, 2000-2001, p. 81.
48 ANAO, Report No.26, 2000-2001, p. 83.
49 ANAO, Report No.26, 2000-2001, p. 62.
50 ANAO, Report No.26, 2000-2001, p. 86.
51 ANAO, Report No.26, 2000-2001, p. 62.
52 ANAO, Report No.26, 2000-2001, p. 86.
53 ANAO, Report No.26, 2000-2001, p. 87.

are in a much better position now to understand exactly what we have in the Estate in comparison to what was the case a few years ago'.

> When we look at the property asset register, one of the activities that we have developed, as part of the creation of the Defence Estate Organisation, is to identify all of the properties and assets.[54]

4.38 Defence went on to say that 'we have a fairly powerful motivator':

> …our contractors get paid based on what work they identify that they are doing. So if they identify an asset or we ask them to do work on it and it is not in our contract, they are going to very quickly identify it so that they can get paid. In this way, we have identified a significant increase in our asset database since we have let the comprehensive maintenance contracts.[55]

Committee comment

4.39 Having considered the evidence, the Committee believes that Defence still has a problem regarding its asset and property registers. While it acknowledges that Defence is making an effort to achieve a full register and link it to ROMANS, the Committee is not satisfied that all the problems have been addressed effectively. It therefore endorses audit recommendation no. 6—'that DEO make better use of its DEMS/FM system in the delivery of its FACOPS Program'—to which Defence has agreed. The Committee believes that Defence should provide greater incentives for REC staff to migrate all their Estate activities fully onto DEMS/FM.

Recommendation 4

4.40 **The Committee recommends that the Defence Estate Organisation facilitate the consolidation of Regional Estate Centre activities fully onto Defence Estate Management System.**

54 B Lane, *Transcript*, 2 May 2001, p. 56.

55 O Hammond, *Transcript*, 2 May 2001, p. 57.

Maintenance benchmark

4.41 ANAO reported that the extent to which repairs and maintenance were carried out on assets was affected by the reduced allocations to the FACOPS Program. Spending was directed to the most essential tasks. This approach in turn affected the capacity of an asset to meet its usage objectives and to retain its valuation. In an attempt to improve matters, DEO has been developing systems to gather firm data so that it may substantiate funding bids and direct spending to essential tasks.[56]

4.42 ANAO calculated that property industry benchmarks for recommended maintenance expenditure show that maintenance of the Defence Estate was underspent by $100m in 2000–2001.[57] This indicated that needed maintenance was being deferred—with significant implications since Defence properties are ageing. In addition to impacting on operational requirements, deferral could also have implications for occupational health and safety and duty of care. The audit cited as supporting evidence 'client dissatisfaction with discretionary funding levels and anecdotal evidence from regional Managers Defence Estate who consistently express concern at the under-funding'.[58]

4.43 When questioned by the Committee about this underspend and the risks which were incurred, Defence agreed that:

> …within Defence in the wider Defence budgetary context we have been under pressure for probably 10 years to establish relative priorities for capability versus support. …we have established priorities not to maintain to the level that might be acceptable in a public arena, some of the assets that do not have a medium or a long-term life in the sense that where we are going to rebuild a base in the short to medium term or where we might adopt a different strategy for how we provide living-in accommodation for personnel, we have chosen not to invest in repairs of those assets.[59]

4.44 Within the context of this risk management strategy for repairs and maintenance, Defence assured the Committee that there 'are

56 ANAO, Report No.26, 2000-2001, p. 40.

57 ANAO, Report No.26, 2000-2001, pp. 40, 95.

58 ANAO, Report No.26, 2000-2001, p. 95.

59 Corey, *Transcript*, 2 May 2001, p. 38.

no instances that I am aware of where any major asset of that nature would be at risk'.[60]

> That is a risk we think we can manage without much difficulty. You may find instances where there are warehouses and storehouses, again because the base has not yet been redeveloped, where some of those assets may pose a risk to the items that are stored in them, but I would suggest to you that they would be only very isolated instances because we have taken the fire prevention measures and others to make sure that we can protect the assets that are inside those buildings to the extent that they need to be protected.[61]

4.45 Defence reiterated that the repairs that were being deferred were repairs on either non-essential assets that Defence had decided had no long-term future or were assets that performed a function where the function may change and be satisfied by a different strategy in the near future.[62]

> We have been prioritising maintenance needs ever since we took over the function from the Department of Administrative Services. There has never been sufficient funding to satisfy all the needs for maintaining buildings. So we have established a planning process where we have a bottom-up and a top-down process that come together at a reasonable level and a central level and where we involve all of the players in the game, apart from private lessees. We make judgments based on capability needs in the first instance and occupational health and safety in the second.[63]

4.46 Questioned about whether any deferrals created a depreciation situation which placed major assets at risk, Defence asserted: 'The assets that are depreciating are probably ones that we will demolish and we will not spend any money on them at all.'[64]

> I would hate to think there were examples of our spending money on something that is being disposed of, but I am sure they probably are out there. The planning

60 Corey, *Transcript*, 2 May 2001, p. 38.
61 Corey, *Transcript*, 2 May 2001, p. 38.
62 Corey, *Transcript*, 2 May 2001, pp. 53–54.
63 Corey, *Transcript*, 2 May 2001, p. 53.
64 Corey, *Transcript*, 2 May 2001, p. 54.

> system we have in place should ensure that that does not happen.[65]

4.47 The Committee wanted to know if the Defence estate was being maintained in accordance with sensible business practices, especially where property may be earmarked for disposal. The Committee asked if any assets were at risk from being housed in properties which were being managed on a risk basis. On both counts, Defence assured the Committee that 'major assets of that nature' were not at risk.[66] Defence explained that repairs were 'done principally on a planning basis'.[67]

> We have part of the repair facilities operations devoted to 'urgent minor maintenance'. About 20 per cent is 'urgent minor maintenance', which you could describe as ad hoc. We would describe it as 'urgent minor maintenance'. It is probably less ad hoc than it is. The rest of it is planned maintenance.[68]

4.48 Defence assured the Committee that maintenance was now based on a needs assessment and no longer simply on funds availability or 'on an ad hoc basis in response to user complaints' when previously scarce maintenance resources had not been well targeted.[69] Defence acknowledged this former unsatisfactory approach in its draft Strategic Plan when it pointed out that in the past 'a spate of mishaps…serves to highlight the risk Defence has taken in arbitrarily cutting maintenance to below industry recommended levels'.[70]

Contract management

4.49 Most of the DEO contracts are in the regions. Each REC manages a different mix of facilities maintenance contracts in old and new forms because of the different contracting arrangements in each region prior to 1997, and from the different knowledge bases and capacities of regional staff. Although DEO allowed a timeframe of

65 Corey, *Transcript*, 2 May 2001, p. 54.
66 Corey, *Transcript*, 2 May 2001, p. 38.
67 Corey, *Transcript*, 2 May 2001, p. 54.
68 Corey, *Transcript*, 2 May 2001, p. 54.
69 ANAO, Report No.26, 2000-2001, p. 92.
70 ANAO, Report No.26, 2000-2001, p. 93.

two to three years for the implementation of recommended changes, most RECs have not totally converted.[71]

4.50 ANAO found that in some cases, formal contracts do not exist—even for work costing over $250 000. In two instances, the contracts had been mislaid for over six months, yet regular payments continued to the contractors. ANAO concluded that 'work awarded without reference to relevant contracts indicates poor contract management'.[72]

Comprehensive maintenance contracts

4.51 Defence told the Committee that DEO had developed comprehensive maintenance contracts throughout the country, thereby replacing the general building/facilities and the fixed plant/equipment maintenance contracts, which ANAO found had been managed poorly.

> The comprehensive maintenance contractors and our focus on planning and managing the contractor rather than actually managing the work will mean that we will be planning our work much more in advance than we did previously…[73]

4.52 Under these contracts—initially for three years with the option to extend a further five, all the necessary personnel and resources to undertake the work specified are the responsibility of the contractors. Contractors are paid an agreed amount to maintain certain agreed standards. ANAO voiced two concerns in its report about these arrangements:

- Because comprehensive maintenance contracts are performance-based, there is an increased risk that only minimal preventative maintenance on fixed plant and equipment would be undertaken.
  - ⇒ The potential for under-maintenance leading to more rapid deterioration, and a shorter life of the asset, forms a major risk.
- A second risk is that such large contracts, when their terms expire, will simply be extended to postpone the tender and

71 ANAO, Report No.26, 2000-2001, pp. 41–43.

72 ANAO, Report No.26, 2000-2001, p. 46.

73 Corey, *Transcript*, 2 May 2001, p. 40.

> assessment process—as had been done in the past—or even allowed to lapse while the work continues.[74]

4.53 The Committee had similar reservations to those expressed by ANAO. It believes that the *Chief Executive Instructions* which are underpinned by the *Financial Management and Accountability Act 1997* should be adhered to during management of contracts. Furthermore, the Committee reiterates that DEO should encourage all its staff to consult the ANAO's *Contract Management Better Practice Guide 2001*. Staff should be aware of their responsibilities when expending Commonwealth funds.

Outputs

4.54 The Committee asked Defence what steps had been taken to implement the audit recommendation that individual facilities' costs be directly linked to the relevant outputs and sub-outputs so that FACOPS program costs can be appropriately attributed to overall Defence outputs. ANAO had found that the costs attributed to outputs were not data-driven but based on management judgement, largely because DEMS/FM was incomplete and not linked to ROMAN.

4.55 Defence had agreed in principle to this recommendation, provided it was practical and cost effective to do so. In its submission, Defence told the Committee:

> Costs for discretionary work, breakdown work and unforeseen maintenance is being captured and attributed to individual assets. Contract fees for maintenance of fixed plant and project management are more difficult to attribute and there is reluctance among our servicing contractors to provide this detail. Negotiations have not been finalised.[75]

4.56 Defence told the Committee that the comprehensive maintenance contracts will allow DEO to identify costs down to building level on a basis which will allow it to attribute directly the costs of maintaining all of the assets of the estate.[76]

---

74 ANAO, Report No.26, 2000-2001, p. 51.

75 Defence, Submission no. 3, p. 3.

76 Corey, *Transcript*, 2 May 2001, p. 53.

ANAO access to contractor records

4.57 The Committee was concerned to read in the audit report that 'none of the facilities maintenance contracts, including recent contracts reviewed in the present audit, provided for suitable Defence or ANAO access'.[77] The Committee had previously recommended in two of its reports that ANAO should be given access to third party premises and records. When asked whether DEO contracts had such access clauses, Defence replied that its recent contracts gave Defence access to view contractor records.

> During the audit, we felt that those contract clauses were adequate for the ANAO to have access; they said that it was not. So we agreed with the ANAO that we would change the clauses in the contract to allow full access.[78]

4.58 The Committee was pleased that Defence has undertaken to insert clauses into future contracts, giving ANAO independent access rather than through Defence. ANAO requires this direct access in order for it to perform its auditing duties.

Staff training

4.59 Staff numbers across DEO, especially in the RECs, have been reduced following the Defence Efficiency Review. ANAO found that the timing of some of these reductions impacted on the standard of contract management in the RECs, particularly where comprehensive maintenance contracts had not been fully implemented.[79] Since some of those exiting were senior military members, DEO feared that it was losing its corporate memory and experience base.[80] The Committee was told that staff remaining in DEO needed to have the appropriate skills and qualifications to manage large, complex contracts in the Defence environment and deliver the services required to fulfil DEO's mission—namely managing the Defence estate to meet Government and defence needs.[81]

4.60 ANAO found that some DEO staff had only limited awareness and ability to apply appropriate procedures relating to the

77 ANAO, Report No.26, 2000-2001, p. 57.
78 Hammond, *Transcript*, 2 May 2001, p. 38.
79 ANAO, Report No.26, 2000-2001, p. 59.
80 ANAO, Report No.26, 2000-2001, p. 54.
81 ANAO, Report No.26, 2000-2001, p. 55.

commitment and expenditure of public money. Instances were cited in the audit report of staff lacking the skills to determine whether contractors had fulfilled their contractual obligations; staff's inability to properly certify monthly invoices for contractor payments; staff exercising delegations without understanding fully their responsibilities; staff unawareness of the need to consult the latest version of *Chief Executive Instructions*; and of staff overspends without approval, totalling $3.8m.[82] Added to this was the low skill level and familiarity with DEMS/FM, DEO's database, among REC staff.

4.61 In its submission, Defence stated that it had undertaken a skill survey and a training team had visited all regions.[83] At the public hearing, Defence said:

> Staff training is a difficult one in that we have been progressively relocating the staff that do not have the skills, that are no longer necessary.…With respect to people that are not capable of being retrained, we are placing them in other positions or giving them the option of finding themselves something else to do.[84]

4.62 ANAO found that DEO had difficulties attracting and retaining appropriately qualified, skilled experienced staff.[85] Defence accepted that it has to review its workforce recruitment, development and retention policies with the aim of ensuring the availability of staff with appropriate qualifications and experience to meet its program objectives. It told the Committee:

> We are progressively implementing a system of recruitment and retention of people. You have got to understand that the sort of skills that we give the people that manage the facilities operations activity and our capital investment program are in high demand outside, and we cannot compete with the private sector. We train them—and they poach them.[86]

4.63 The Committee is aware of Defence's poor record in contract and project management, and is of the view that Defence still has a long way to go before DEO staff are able to effectively exercise

82 ANAO, Report No.26, 2000-2001, pp. 48–49, 52–3, 75, 77.

83 Defence, Submission no. 2, p. 5.

84 Corey, *Transcript*, 2 May 2001, p. 55.

85 ANAO, Report No.26, 2000-2001, p. 55.

86 Corey, *Transcript*, 2 May 2001, p. 55.

their responsibilities for properties and assets with a gross replacement value of $14.8 billion. Staff need to be motivated to develop the abilities to prioritise timely maintenance, develop sound business practices and the skill to manage contractors. Defence needs not only to hone its performance indicators to reflect these skills but needs also to implement appropriate manpower replacement strategies.

Recommendation 5

4.64 **The Committee recommends that Defence review its performance indicators for Defence Estate Organisation staff so that staff are encouraged to develop essential management and financial skills.**

Financial management

4.65 Although DEO is supposed to deliver estate services on a priority basis by region rather than by individual establishment, this does not always occur.[87] ANAO analysis, based on final allocation and expenditure data for 1999–2000 rather than on the RECs' proposed works programs, indicated that there was limited alignment between approved budget allocations and actual expenditure. The audit found some significant mismatches between allocation and expenditure in the samples tested.[88]

4.66 DEO Central Office issued some 26 Allocation Variation Advice notices to RECs over the financial year. ANAO commented: 'The value of continual allocation advice provided to the RECs is questionable if compliance with the advice is not mandatory.'[89]

> The work by the RECs in developing detailed bids and by EOP Branch in consolidating the bids, allocating funds and monitoring expenditure becomes nugatory if RECs can shift funds to lower priority work.[90]

4.67 Currently, funds allocated to RECs are at times spent on lower priority work without consultation and agreement by Central

87 ANAO, Report No.26, 2000-2001, p. 12.
88 ANAO, Report No.26, 2000-2001, pp. 71–73.
89 ANAO, Report No.26, 2000-2001, p. 74.
90 ANAO, Report No.26, 2000-2001, p. 74.

Office. While accepting the need for flexibility given the scale of the Program, ANAO believes it is important that there be clear understanding and communication between the RECs and Central Office in order to ensure effective management and oversight of the pre-determined priorities.[91]

4.68 Because regular two-way consultation between DEO and some clients did not occur, this impacted adversely on DEO's ability to efficiently and effectively deliver the FACOPS Program, and on associated client satisfaction.

4.69 The reduced resources allocated to the FACOPS Program resulted in DEO developing systems such as Total Estate Management to gather firm data on the condition of the Estate that are needed to substantiate funding bids and to direct spending to essential tasks. Total Estate Management considers the entire asset life-cycle within a framework of strategic planning and management guidance. It aids resource management both in terms of analytical justification of proposals and better targeting of scarce resources.[92]

End of year spending

4.70 The Committee questioned Defence on its practice of pressing the RECs to spend all their funds before the end of the financial year, thus resulting in a spending rush in May and June. This practice was contrary to the *Chief Executives Instructions*. ANAO had concluded that 'the practice of exhausting appropriations before they lapse is undesirable unless there is a commensurate advantage for the Commonwealth'.

> So much expenditure in such a short time raises concerns that projects are chosen, designed and delivered in haste, and that the Commonwealth may therefore not be receiving value for money. It is also unclear how so many projects being managed in such a short time frame can be managed effectively.[93]

4.71 Defence explained that under the previous accounting regime, it was penalised significantly because of the way its budget was structured. The following year's budget was based on its total expenditure in the previous year. 'If we did not achieve it, we

91 ANAO, Report No.26, 2000-2001, p. 79.
92 ANAO, Report No.26, 2000-2001, p. 33.
93 ANAO, Report No.26, 2000-2001, p. 75.

were penalised. We were doubly penalised: we did not spend it in the year in which we had it and we did not get it the next year as well.'[94]

4.72 Defence assured the Committee that the present expenditure pattern is changing because DEO has a different way of contracting for work.

> Under the new regime which we have now, with the comprehensive maintenance contracts in place throughout the country, we expect that that pattern will go away....we will be planning our work much more in advance than we did previously, so expenditure will occur in a much more stable pattern across the year. There will probably still be some elements of trending up expenditure as the year progresses, just because of the nature of the way the orders are placed. We are fighting that, and it is something we have been fighting for as long as I have been around the organisation. With the new contracts and the new emphasis on planning, we anticipate that we will win that battle.[95]

4.73 Defence further explained that although orders may be placed progressively throughout the year, in reality, a lot of the work did not get placed until after the first or second quarter so the work was done around the country in the third and fourth quarters.

> While it looks like you are rushing around and spending money for the sake of spending money at the end of the financial year, that is not the case…With the new accounting arrangements, the accrual budgeting arrangements, the incentive to achieve your cash budget is not as great as it was previously.[96]

4.74 DEO told the Committee it was trying to encourage its staff to place orders before July so that contractors can commence in July. However, there is some staff resistance to this.[97] It has also moved advanced approval of projects to February-March of the preceding financial year to allow some documentation to be done, working on the basis of securing 70 per cent of their forward estimates. DEO expects this new approach will produce a more even

94 Corey, *Transcript*, 2 May 2001, p. 40.
95 Corey, *Transcript*, 2 May 2001, p. 40.
96 Corey, *Transcript*, 2 May 2001, p. 40.
97 Corey, *Transcript*, 2 May 2001, p. 41.

expenditure pattern thereby replacing the sudden leaps towards the end of the financial as in the past. 'But, again, design cannot be fully committed until the new financial year. That means we will get a slight J-curve but the gradient should improve after that.'[98] Unexpected emergencies such a cyclone or a flood would require that DEO's program be adjusted accordingly.

Sale and lease-back

4.75 When the Committee questioned Defence about its sale and lease-back arrangements and the extent these represented value for money relative to the Commonwealth continuing to own those assets itself, Defence responded: 'The government made a judgment that the sale and lease-back of those properties was in the best interests of the government.'[99]

4.76 Asked to elaborate, Defence commented:

> From where we sat in Defence we felt that some were marginal cases and others were less marginal. In a whole of government context, there may have been a different perspective put on it.
>
> …on the basis that Defence would be occupying the building for perhaps 50 years, we thought that it did not make a great deal of economic sense from a Defence perspective to sell them and lease them back.[100]

4.77 The Committee was told the government agreed to supplement Defence for the costs of the lease-back of those sales that did not make sense from a Defence perspective.[101] Other arrangements were entered into, especially regarding the sale of buildings such as the Russell complex and Campbell Park which 'will be necessary for as long as we can see into the future'.[102]

Retaining a percentage of the proceeds of property sales

4.78 The Committee was informed that the sale of Defence properties dated back to 1989, when the former Department of Administrative Services no longer looked after Defence properties.

98 Hammond, *Transcript*, 2 May 2001, pp. 41–42.
99 Corey, *Transcript*, 2 May 2001, p. 46.
100 Corey, *Transcript*, 2 May 2001, p. 46.
101 Corey, *Transcript*, 2 May 2001, p. 47.
102 Corey, *Transcript*, 2 May 2001, p. 47.

> …there was an agreement of Cabinet at that time that we could, to give Defence an incentive to dispose and rationalise some of its properties, retain up to one per cent of the net revenue from disposal of Defence properties—that is, one per cent of Defence outlay. In today's terms, that is probably some $150 million or $160 million a year. That was in place until last year.[103]

4.79 Questioned further, Defence explained:

> There was no overall cap. It was just one per cent, and above one per cent we shared the proceeds fifty-fifty with the broader budget. If we achieved revenue of more than one per cent of Defence outlay, and say Defence outlay was $15 billion so it would be $150 million, then if we achieved $200 million we would retain $150 million and beyond that we would share fifty-fifty with the broader budget.[104]

4.80 The incentive came from having this amount 'added on to Defence budget funding; it was not part of Defence budget funding. The Defence budget was $11 billion, plus any revenue from return of sales, up to one per cent.'[105]

4.81 When the Committee asked why Defence had originally needed an incentive to sell property, it was told that the Defence culture had had to be changed.

> Within the Defence organisation, properties that the Army were on were [regarded as] Army properties and properties that the Navy were on were Navy properties, and they were not going to move for any reason.[106]

4.82 Since then, however:

> Everyone within Defence understands that they have to make maximum use of the resources, whether those resources are in terms of property or whatever. We have moved from 500 plus properties in 1991 to 380 now and there is a further 100 for disposal. Prior to 1990, we would probably have been lucky to dispose of 10 properties in the history of Defence.[107]

---

103 Corey, *Transcript*, 2 May 2001, p. 48.
104 Corey, *Transcript*, 2 May 2001, p. 48.
105 Corey, *Transcript*, 2 May 2001, p. 48.
106 Corey, *Transcript*, 2 May 2001, p. 51.
107 Corey, *Transcript*, 2 May 2001, p. 51.

4.83 In 2000, the Government specified Defence properties where Defence was not to retain any revenue from the sales. Instead, the sale revenue was returned directly to the budget. 'That was $500 million worth of property sales identified in last year's budget.'[108]

> In the Expenditure Review Committee of Cabinet last year [2000] and in the budget it was determined that the revenue from disposal of properties would be determined in the annual review of the Defence budget. In any one year the government left itself the flexibility either to let us retain the one per cent or to direct it to the general budget.[109]

4.84 In the 2001–2002 Budget, Defence identified $634 million as the amount 'for sale of assets' returned to DoFA—namely to consolidated revenue.[110] The Defence *Portfolio Budget Statement, 2001–2002* stated that $241 million from property sales will be allocated to Defence, 'in addition to the forward estimates and in addition to the White Paper funding increases'.[111] It was projected that the allocated amount from sales will be $131.3m in 2002–2003, $135m in 2003–2004, and $140.5m in 2004–2005.[112] Defence will continue to be provided with rental supplementation in respect of commercial rent charged on leased back properties.

Committee comment

4.85 The Committee was satisfied that Defence has made an effort to spread its future expenditure over the full financial year. Matters could be improved were Defence to give a higher priority to financial and managerial training for all its REC staff.

Bob Charles MP
Chairman
29 August 2001

108 Corey, *Transcript*, 2 May 2001, p. 49.
109 Corey, *Transcript*, 2 May 2001, p. 50.
110 Defence, Submission no. 9, p. 1.
111 Defence, *Portfolio Budget Statement, 2001–2002*, Commonwealth of Australia 2001, p. 20.
112 Defence, *Portfolio Budget Statement, 2001–2002*, p. 20.

A

Appendix A — Conduct of the Committee's review

Selection of audit reports

The Auditor-General presented eighteen reports in the second and third quarters of 2000–2001. These were:

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

- No. 13 Performance Audit
  Certified Agreements in the Australian Public Service
  Across Agencies

- No. 14 Information Support Service
  Benchmarking the Internal Audit Function
  Across Agencies

- No. 15 Performance Audit
  Agencies' Performance Monitoring of Commonwealth Government Business Enterprises
  Across Agencies

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

- No. 17 Performance Audit

  Administration of the Waterfront Redundancy Scheme
  Department of Transport and Regional Services, Maritime Industry Finance Company Ltd

- No. 18 Performance Audit

  Reform of Service Delivery of Business Assistance Programs
  Department of Industry Science and Resources

- No. 19 Financial Control and Administration Audit

  Management of Public Sector Travel Arrangements—Follow-up audit
  Across Agencies

- No. 20 Performance Audit

  Second Tranche Sale of Telstra Shares
  OASITO

- No. 21 Performance Audit

  Management of the National Highways System Program
  Department of Transport and Regional Services

- No. 22 Performance Audit

  Fraud Control in Defence
  Department of Defence

- No. 23 Financial Statement Audit

  Audits of the Financial Statements of Commonwealth Entities for the Period Ended 30 June 2000
  Across Agencies

- No. 24 Performance Audit

  Family Relationships Services Program
  Department of Family and Community Services

- No. 25 Information Support Service

  Benchmarking the Finance Function
  Across Agencies

- No. 26 Performance Audit

  Defence Estate Facilities Operations
  Department of Defence

- No. 27 Performance Audit

  Program Administration in Training and Youth Division—Business Process Reengineering
  Department of Education Training and Youth Affairs

- No. 28 Audit Activity Report

  July to December 2000—Summary of Outcomes 2000/2001
  Across Agencies

- No. 29 Performance Audit

  Review of Veterans' Appeals Against Disability Compensation Entitlement Decisions
  Department of Veterans' Affairs

- No. 30 Performance Audit

  Management of the Work for the Dole Program
  Department of Employment, Workplace relations and Small Business

The Joint Committee of Public Accounts and Audit discussed the above audit reports and considered whether the issues and findings in the reports warranted further examination at a public hearing. In making this assessment the Committee considered, in relation to each audit report:

- the significance of the program or issues canvassed in the audit report;
- the significance of the audit findings;
- the response of the audited agencies, as detailed in each audit report, and
- the extent of any public interest in the audit report.

Following this consideration, the Committee decided to take evidence at public hearings on the following audit reports:

- Audit Report No. 16 Performance Audit
  Australian Taxation Office Internal Fraud Control Arrangements;
- Audit Report No. 22 Performance Audit
  Fraud Control in Defence; and
- Audit Report No. 26 Performance Audit
  Defence Estate Facilities Operations.

The evidence

The Committee held public hearings in Canberra on 2 May 2001. The transcript of evidence taken at the hearings is reproduced at Appendix C.

B

Appendix B — Submissions & Exhibits

Submissions

No.	Individual/Organisation
1	Department of Defence
2	Department of Defence
3	Department of Defence
4	Australian Taxation Office
5	Australian Taxation Office
6	Department of Defence
7	Department of Defence
8	Department of Defence
9	Department of Defence

Exhibits

No.	Individual/Organisation and Title
1.	Australian Taxation Office, *Report of an Internal Review of the Systems and Procedures relating to Private Binding Rulings and Advance Opinions in the Australian Taxation Office*, May 2001
2.	Australian Taxation Office, *The integrity of the Private Binding Rulings System*, May 2001
3.	Australian Taxation Office, *Specific Recommendations and Responses from the Sherman Review*, May 2001

C

Appendix C — Transcript of evidence