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.