Protection of Confidential Client Data from Unauthorised Disclosure

Department of Social Security
Centrelink

ISSN 1036-7632

ISBN 0 644 39192 8

Canberra ACT
20 March 1998

Dear Madam President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit of the Department of Social Security and Centrelink, in accordance with the Authority contained in the *Auditor-General Act 1997*. I present this report and the accompanying brochure to the Parliament. The report is titled *Protection of Confidential Client Data from Unauthorised Disclosure.*

Yours sincerely

P. J. Barrett
Auditor-General

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

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

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

The Publications Manager
Australian National Audit Office
GPO Box 707 Canberra ACT 2601
telephone (02) 6203 7537
fax (02) 6203 7798

Information on ANAO audit reports and activities is available at the following Internet address:

http://www.anao.gov.au

Audit Manager

Margaret Rahmann
Malisa Golightly
Sue Sheridan

Abbreviations/Glossary

ADP	Automated Data Processing
AFP	Australian Federal Police
ANAO	Australian National Audit Office
CBT	Computer Based Training
Centrelink	The new Commonwealth services delivery agency
CR&R	Control, Review and Recovery
CRAM	Client Record Access Monitor
CSDA	Commonwealth Services Delivery Agency
DAF	Deny Access Facility
DEETYA	Department of Employment, Education, Training and Youth Affairs
DHFS	Department of Health and Family Services
DPP	Director Public Prosecutions
DSS	Department of Social Security
FIRECALL	A facility which allows access to mainframe resources which are normally disallowed by computer security
FOI	Freedom of Information
HIC	Health Insurance Commission
ISIS	Income Security Integrated System
ISS	Income Security Systems
IT	Information Technology
PAS	Privacy Allegation System
PFS	Protective File System
SAMS	Security Access Management System
SMS	Security Monitor System
SPC	Security and Privacy Committee
SSP	Strategic Security Project

Part One

Summary and Recommendations

Summary

Introduction

1. The confidentiality provisions of the Social Security Act 1991 expressly forbid the release of customer information except in very limited circumstances which are prescribed by the legislation or set out in Ministerial guidelines laid before the Parliament. The improper disclosure of 'customer' or 'client' information by staff and the soliciting of such information from staff are matters of serious concern to the Department of Social Security (DSS) and Centrelink.

2. Audit Report No.23 1993-94 *Protection of Confidential Client Information from Unauthorised Disclosure,* tabled in Parliament in December 1993, examined the efficiency and effectiveness of the management and implementation of the protection of confidential client information from unauthorised disclosure within DSS. The ANAO acknowledged DSS' strong commitment to the protection of client information from unauthorised release, and that DSS had implemented a range of measures to strengthen data confidentiality. Nevertheless, the ANAO identified scope for further improvement in the following major areas:

- the assessment of the risk of unauthorised disclosure of client information;
- checks and controls on access by staff to client data;
- the strategic management of confidentiality issues;
- operational strategy for the protection of client data, such as the staff pre-employment checks and initial training; and
- Information Technology (IT) systems and controls over client data, including the access by specialist IT staff to client data in IT production.

Follow-up audit objective

1. The purpose of this follow-up audit was to report on action taken by DSS and Centrelink in addressing the recommendations of Audit Report No.23 1993-94 *Protection of Confidential Client Information from Unauthorised Disclosure*. The objectives were to:

- ascertain the extent to which the recommendations of the original audit have been implemented;
- identify other changes made in relation to data confidentiality within the Social Security portfolio since 1993;
- assess the impact of the changes made; and
- identify any scope for further improvement.

2. It is particularly timely to undertake the follow-up audit as recent developments have focused public interest on issues of confidentiality. These include:

- the separation of policy departments from service delivery through developments such as the setting up of Centrelink and a competitive employment services market[1]; and
- the Government decision to out-source most Commonwealth Government Information Technology processing.

Follow-up audit approach

1. There were 42 recommendations in the original audit. In undertaking the follow-up audit, the ANAO took into account the reports forwarded by the Minister for Social Security to the Minister for Finance (March and September 1994) regarding progress made against these recommendations together with updates from DSS and Centrelink on action taken to date in relation to each recommendation.

2. In order to focus the ANAO's examination effectively on the central concerns, a sample of 14 recommendations was selected for further follow-up review. The selection of recommendations to be included in this sample was undertaken in a way which ensured coverage of all the major areas identified in the original report, with the exception of those relating to the strategic management of the protection of client data. The recommendations within this theme relate mainly to the role and function of the former DSS Privacy Branch. Given the major structural changes which directly affected this Branch, among others, that were underway with the transition to Centrelink at the time of the audit fieldwork, the ANAO did not consider that it was feasible to follow-up these recommendations.

---

[1] At the time of writing this report, a tender let by DEETYA for employment services had closed. Successful tenderers will be subject to privacy regulations under the proposed terms of the contract, which is expected to be in operation from 1 May 1998.

3. In the event, because most of the recommendations were interlinked, the evidence gathered in undertaking this testing also enabled the ANAO to make an indicative assessment of action against many of the remaining recommendations. Appendix 1 summarises the ANAO's assessment, and the basis for that assessment, for each recommendation.

Overall Conclusion

1. DSS and Centrelink have implemented, and in some cases extended, many of the ANAO's 1993 recommendations, in particular the full logging of staff access to customer data. However, despite this and many other positive initiatives, the number of substantiated allegations against staff of unauthorised disclosure of client information has not decreased in the last three years. This points to the need for further improvement in the management of privacy concerns.

2. In particular, the ANAO considers that Centrelink should:

- significantly improve the analysis of the details of both the alleged and substantiated breaches of privacy to determine factors leading to increases or trends in the number of instances reported and confirmed;
- review its management strategy in the light of this analysis and take action to counter the perceived risks; and
- monitor the outcomes of these actions more rigorously than in the past.

Recommendations and responses

1. The ANAO has made a number of recommendations to build on the improvements to date and to ensure that the full intent of the original recommendations (made in the 1993-94 report) is understood and appropriate action taken.

2. DSS and Centrelink have agreed with all recommendations. DSS noted that the recommendations of the follow-up audit relate primarily to the operations of Centrelink.

3. Centrelink indicated that it is committed to implementing the ANAO's recommendations about protection of customer information as quickly as possible.

Key Findings

4. The ANAO considers that action taken by DSS and Centrelink have satisfied the requirements of those recommendations contained in the original report which referred to:

- increased use and monitoring of audit trails to detect unauthorised access to customer data by network staff;
- increased support for Privacy Officers and investigators of allegations; and
- improvements to systems designed for customers needing enhanced protection.

5. Improvements have also been made to the provision of privacy awareness training to new staff. However, the ANAO found that a significant number of the staff interviewed during the audit had not yet received formal training in the area. There was also evidence that not all staff were completing the computer-based training packages developed for privacy awareness training. Therefore, the ANAO considers that there are opportunities for Centrelink to improve attendance at formal training courses, where cost effective, or explore other appropriate strategies for ensuring that all staff are fully aware of their responsibilities with regard to the strict confidentiality provisions of the Social Security Act and take appropriate action.

6. In order to minimise the risk of unauthorised access and use of customer information the ANAO has identified scope for further improvements as follows. Centrelink should:

- significantly improve the analysis of data on alleged and substantiated privacy breaches in order to assess the effectiveness of current data protection initiatives and develop additional strategies for further reducing the risk of breaches;
- ensure full compliance with the policy and guidelines on pre-employment checks;
- improve the security of customer data by significantly increasing the use of reports which are targeted at monitoring IT staff access to this data; and

- develop appropriate strategies for protecting customer information during testing changes to the IT system in order to comply fully with the legislative requirements of privacy and confidentiality.

7. The ANAO has made six recommendations for improvement in the areas listed above.

Recommendations

Set out below are the ANAO's recommendations, with report paragraph reference and the agencies' abbreviated responses. More detailed responses are shown in the body of the report.

Recommendation No.1 Para. 2.28

The ANAO *recommends* that Centrelink takes further action to provide all officers, including temporary officers, with a sound understanding of their privacy obligations including through the provision of privacy awareness courses shortly after joining Centrelink, with refresher courses at regular intervals, or through other appropriate strategies where the provision of formal courses is not cost effective.

Centrelink response: Agreed

DSS response*:* Agreed

Recommendation No.2 Para. 3.22

In order to provide a basis for measuring the success of, and revising where necessary, strategies implemented with the aim of minimising unauthorised access to, and disclosure of, confidential information, the ANAO *recommends* that Centrelink:

- ensures that information currently collected in relation to alleged and substantiated breaches of privacy is comprehensively analysed;
- undertakes a cost/benefit analysis to determine the feasibility of extending the existing Privacy Allegations System to include further details concerning these allegations in order to identify potentially high risk areas, and provide an enhanced understanding of identified trends so that appropriate action can be taken in a timely manner; and
- ensures that the commentary on the analysis of information collected for the quarterly and

annual reports to the Security and Privacy Committee addresses key performance issues, including an analysis of any significant trends identified over longer periods of time.

Centrelink response: Agreed

DSS response*:* See Centrelink response

Recommendation No.3 Para. 3.26

The ANAO *recommends* that Centrelink develops a consistent format for reporting details of privacy allegations and investigations in its Annual Report that would enable the Parliament and the public to better assess, and discern significant trends in, its performance**.**

Centrelink response: Agreed

DSS response: See Centrelink response

Recommendation No.4 Para. 3.41

The ANAO *recommends* that Centrelink takes action to ensure that:

- all Centrelink offices comply with the policy and guidelines in relation to pre-employment checking of prospective staff;
- persons seeking employment with Centrelink are required to sign the release to obtain information in advance of any prospective employment and that requests for checks are referred promptly to the Australian Federal Police; and
- all necessary documentation is checked prior to employment.

Centrelink response: Agreed

DSS response*:* Agreed

Recommendation No.5 Para. 3.51

The ANAO *recommends* that:

- Centrelink investigates the cost-effectiveness of implementing targeted monitoring of programmer access to the production database, as part of the Strategic Security Project; and
- the use of FIRECALL privileges be monitored regularly**.**

Centrelink response: Agreed

DSS response: See Centrelink response

Recommendation No.6 Para. 3.63

The ANAO *recommends* that, in order to comply fully with the legislative requirements of privacy and confidentiality, Centrelink explore alternative strategies for protecting data during testing, including the option of using outside expertise, if the Data Scrambling project is found to be prohibitively difficult or expensive.

Centrelink response: Agreed

DSS response*:* See Centrelink response

Part Two

Audit Findings and Conclusions

Introduction

This is a follow-up audit of the actions of the Department of Social Security and Centrelink in addressing the ANAO's recommendations made in Audit Report No.23 1993-94. This chapter outlines the background to this follow-up audit including the original audit findings, recent changes to the Social Security Portfolio, and the audit methodology.

Background to the audit

1.1 Audit Report No.23 1993-94 *Protection of Confidential Client Information from Unauthorised Disclosure,* tabled in to Parliament in December 1993, examined the efficiency and effectiveness of the management and implementation of the protection of confidential client information from unauthorised disclosure within the Department of Social Security (DSS). The ANAO acknowledged DSS' strong commitment to the protection of client information from unauthorised release, and that DSS had implemented a range of measures to strengthen data confidentiality. Nevertheless, the ANAO identified scope for further improvement in the following major areas:

- the assessment of the risk of unauthorised disclosure of client information;
- checks and controls on access by staff to client data;
- the strategic management of confidentiality issues;
- operational strategy for the protection of client data, such as the staff pre-employment checks and initial training; and
- Information Technology (IT) systems and controls over client data, including the access by specialist IT staff to client data in IT production.

1.2 Audit Report No.23 contained 42 recommendations for improvement. These recommendations together with DSS' responses are shown in Appendix 1 to this report.

Operating environment

Changes to the Social Security Portfolio

1.3 The Commonwealth Services Delivery Agency, known as Centrelink, is a statutory authority, in the Social Security portfolio, established on 1 July 1997 to provide a wide range of Commonwealth Government services to the

Australian community. Centrelink delivers all payments and services previously provided by DSS, together with some services from the Department of Employment, Education, Training and Youth Affairs (DEETYA) and the Department of Health and Family Services (DHFS), with the administration of Childcare Rebates transferred from the Health Insurance Commission (HIC). The functional responsibility for many of the issues addressed by the recommendations of the 1993 audit now reside with Centrelink rather than with the DSS.

Structure of Centrelink

1.4 In June 1996, DSS employed a total staff of 20 000 and was structured as follows:

- a National Administration in Canberra;
- 19 Area Offices, each supporting a number of Regional Offices;
- 216 Regional Offices throughout Australia; and
- a number of smaller offices, managed by Regional Offices.

1.5 Centrelink operates under a similar structure, that is, a National Support Office, and a network of Area and local offices has been established for Centrelink. DSS, which is responsible for policy, housing services programs, and the management of service arrangements with Centrelink, now has staff (600) located at National Office only.

1.6 Staffing in Centrelink has been made up of approximately 20,000 staff transferred from DSS and 3,000 from DEETYA. The Area, Regional and smaller offices are referred to within DSS and Centrelink as 'the network'.

1.7 As part of the establishment of Centrelink, the Administrative Law Branch of DSS, which includes the Privacy Section, has been brought into the Compliance, Fraud and Teleservice Division of Centrelink. Therefore the Security and Privacy Sections are now both in the one Division, within Centrelink.

Data sharing between Commonwealth Government agencies

1.8 Although the relevant Commonwealth departments still have responsibility for providing policy advice in discrete areas, Centrelink has responsibility for delivering a range of services in accordance with Government policy service agreements with purchaser departments. Centrelink staff will potentially have access to customer data which was originally provided to DSS, DEETYA, DHFS or the HIC.

1.9 There has been a recognition by managers in the establishment of Centrelink that the new agency will need to comply fully with the principles underlying the Privacy Act. This recognition was underlined by a public commitment from the Minister for Social Security to undertake the development of guidelines on the privacy principles in consultation with the Privacy Commissioner (see Figure 1 below).

Figure 1

As part of the consultation process, . . .I have agreed to make a public commitment on the privacy issue, and I am happy to give such a commitment. The government has consistently stressed that the existing privacy regime, including the Privacy Act, will apply to the Services Delivery Agency and there will be no diminution in the protection that the Privacy Act and the confidentiality provisions of the Social Security Act, for example, affords to customers of the agency. While the agency will be subject to the Privacy Act, I want to ensure that the bringing together of the functions of several departments fully complies with the principles underlying the Privacy Act.

I intend that the agency and the departments involved will consult with the Privacy Commissioner in the development of guidelines. I will subsequently direct the board of the agency to follow these guidelines.

Senator Newman speaking to the Bills establishing the CSDA, 26 March 1997
Hansard page: 2181

Security and Privacy Committee

1.10 The key area with responsibility for privacy and security within the Social Security portfolio is that of the Security and Privacy Committee (SPC), a senior management committee. The SPC meets quarterly to consider issues of privacy and security and to decide policy, to supervise initiatives underway and to monitor reports from the sections responsible for analysing allegations and the results of investigations. The SPC has continued to operate since the establishment of Centrelink.

Follow-up audit objective

1.11 The purpose of this follow-up audit was to report on action taken by DSS and Centrelink in addressing the recommendations of Audit Report No 23 1993-94 *Protection of Confidential Client Information from Unauthorised Disclosure*. The objectives were to:

- ascertain the extent to which the recommendations of the original audit have been implemented;
- identify other changes made in relation to data confidentiality within the Social Security portfolio since 1993;
- assess the impact of the changes made; and
- identify any scope for further improvement.

1.12 It is particularly timely to undertake the follow-up audit, as recent developments have focused public interest on issues of confidentiality. These developments include:

- the separation of policy departments from service delivery through developments such as the setting up of Centrelink and a competitive employment services market[2]; and
- the Government decision to outsource most Commonwealth Government Information Technology processing.

Follow-up audit approach

1.13 There were 42 recommendations in the original audit. In undertaking the follow-up audit, the ANAO took into account the reports forwarded by the Minister for Social Security to the Minister for Finance regarding progress made against these recommendations. Two such reports, in March 1994 and September 1994, have been prepared, indicating finalisation or no intention to act on 20 of these recommendations. Of the balance, up to that time DSS had indicate action or intend to action a further 17 recommendations. Given the elapsed time since the last of these reports, the ANAO sought updates from DSS and Centrelink on action taken to date in relation to each recommendation.

---

[2] At the time of writing this report, a tender let by DEETYA for employment services had closed. Successful tenderers will be subject to privacy regulations under the proposed terms of the contract, which is expected to be in operation from 1 May 1998.

1.14 In order to focus the ANAO's examination effectively on the central concerns, a sample of recommendations was then selected for further follow-up review. The selection of recommendations to be included in this sample was undertaken in a way which ensured coverage of all the major themes identified in the recommendations of the original audit, with the exception of those relating to the strategic management of the protection of client data. The recommendations within this theme relate mainly to the role and function of the former DSS Privacy Branch. Given the major structural changes which directly affected this Branch, among others, underway with the transition to Centrelink at the time of the audit fieldwork, the ANAO did not consider that it was feasible to fully follow-up these recommendations.

1.15 In addition, the ANAO ensured that the sample included a selection of recommendations which had been reported to the Minister for Finance as being finalised as well as those which were still being actioned. The ANAO also ensured that each of the main areas which had responsibility for implementing the recommendations was tested (for example, National Support Office or managers within the network).

1.16 Based on this criteria, 14 recommendations were selected for follow-up review. In the event, because most of the recommendations were interlinked, the evidence gathered in undertaking this testing also enabled the ANAO to make an indicative assessment of action against many of the remaining recommendations. Appendix 1 summarises the ANAO's assessment, and the basis for that assessment, for each recommendation.

Fieldwork

1.17 The majority of the fieldwork was conducted at the National Support Office of Centrelink in those areas responsible for data security, with the administration of privacy legislation and with the implementation of Information Technology. In the network, three Area Offices and six Regional Offices were included in the audit.

1.18 The audit was conducted in close contact with ANAO financial statement auditors because of the implications of data integrity with respect to the financial statement audit.

The Report

1.19 In Chapter 2, the ANAO describes significant improvements made since the original report. In Chapter 3, the ANAO addresses in detail the four

areas in which Centrelink needs to reduce risk further and makes recommendations for improvements in these areas.

1.20 Appendix 1 provides a summary of the ANAO's findings in relation to each of the original recommendations. In accordance with the audit approach described above, some of these findings have resulted from follow-up testing, while others are an indicative assessment only. The basis for the assessment is clearly marked against each recommendation. The Appendix also includes cross-references to Chapters 2 and 3 where selected issues are discussed more fully.

1.21 The audit was conducted in accordance with the ANAO Auditing Standards at a cost of $89 600.

2. Improvements since the 1993 audit

This chapter describes the significant action taken by DSS and Centrelink to address the recommendations of the original report in relation to the increased use and monitoring of audit trails to detect unauthorised access, privacy training, support for Privacy Officers and investigators and improvements to systems designed for customers needing enhanced protection. The ANAO concludes that the intent of the original recommendations has been satisfied in all these areas except in relation to privacy training for new staff. While this training has improved significantly, the ANAO considers that there are opportunities for Centrelink to increase attendance at formal training courses where cost effective.

Introduction

2.1 As mentioned in Chapter 1, the ANAO's audit approach involved examining the major themes for improvement identified in the original report. In relation to three of these areas DSS and Centrelink have taken significant action to address the intent of the original recommendations. These three areas were:

- increased use of audit trails and subsequent monitoring of access to customer data by network staff to detect instances of unauthorised access;
- early training in privacy awareness for all new staff and increasing the level of support for Privacy Officers and investigators of allegations; and
- improvements to the Protective File System which aimed to deter unauthorised access to information relating to customers who were 'at risk'.

Development of comprehensive audit trails and associated monitoring systems

Issues identified in the original audit

2.2 Audit trails are records, or 'logs', of computer transactions. The purpose of implementing an audit trail is to enable effective monitoring and

analysis of user accesses to the computer system, to functions and to data in order to determine whether the access was authorised. Computer operating systems provide this facility at a range of levels and each organisation has to make a decision regarding which level it wants to implement. An example of a very basic audit trail would be a record of who had logged on, with the times of logon and logoff. More extensive logging comes at greater cost, for example, there may be requirements for more computer disc space and increased processing capacity so that response times are not degraded. The decision on whether logs should be minimal, comprehensive, or somewhere in between, is a business decision based on balancing costs against the benefits to the organisation.

2.3 At the time of the original audit, DSS recorded logon access and minimal transaction information. This restricted audit trail did not record the individual user's actions while logged on, including the records that had been viewed. If an allegation of a breach of privacy was being investigated, a more comprehensive trail could then be initiated to record the user identification, client, type of access and time of day. The more comprehensive audit trail could be placed on either a particular customer's record or a particular staff member's user identification, but this was only after the allegation had been made. DSS's capability to check who had improperly accessed and used customer data was very limited as a comprehensive log of such information was not available.

2.4 In its 1993 report the ANAO recommended (Recommendation No. 3) that DSS conduct a cost/benefit analysis to determine the feasibility of logging all, or an increased percentage of, accesses to client data, in order to provide evidence if required, but also as a deterrent measure. In its response, DSS agreed with the recommendation but commented that it would look "to a more cost effective and practical solution than slavishly logging all accesses".

Follow-up audit findings

2.5 Since the audit report, there have been two key developments which have contributed to the implementation of the intent of the ANAO's recommendations in this area. These are the implementation of:

- logging all accesses to client data (referred to as full logging); and
- a system to monitor the information collected through full logging of accesses. This system is known as the Security Monitor System (SMS).

2.6 These are described in more detail below.

Full logging

2.7 With advances in computer technology, the cost of storing computer data has dropped dramatically in recent years, and huge quantities of data can now be stored on-line relatively cheaply and quickly accessed when required. DSS and Centrelink have been able to take advantage of this lowered cost to provide faster processing of customer data, and also to implement the option of full logging of all accesses to that data. All access to customer data on the Income Security Integrated System (ISIS)[3] has been fully logged since February 1994. The logs are indexed for quick retrieval, are stored on-line, and provide a complete audit trail when the need arises.

Security Monitor System - Client Record Access Monitoring (CRAM) reports

2.8 Logging the information is, however, only part of the solution. This logged information also needs to be easily accessible or it will be of little use. DSS has developed the Security Monitor System (SMS) to provide that easy access. A small number of authorised users (mainly Privacy Officers though this varies between Area Offices) access the logs through the SMS. They use these logs early in the investigation of alleged breaches of confidentiality.

2.9 When an allegation of a breach of confidentiality is received, either in relation to a particular customer or against a named staff member, as a standard procedure Privacy Officers, or other authorised investigating officers, specify a timeframe and then run reports which list:

- all accesses to a particular customer's record with the details of the logon ID of the user and the times; and
- the customer records a particular staff member has looked at, with details of which screens were looked at and the exact times.

2.10 These reports are known as *Client Record Access Monitor* (CRAM) reports. The investigating officers use the CRAM reports as the basis of their analysis against the duties of the officers involved. The reports may provide evidence that a staff member has browsed a record without authority and, in this case, the inquiry will continue. Alternatively, the investigating officer can clear a staff member against whom an unfounded allegation had been made.

---

[3] DSS and Centrelink are gradually migrating the computer systems which record and process program payments to a common architecture as part of the Income Security Integrated System (ISIS). The systems will share information on clients through access to a common module known as Customer Registration. Other IT modules, such as Debt Management and Advices will also be shared across the payment systems.

2.11 Authorised staff within the Security Section in Centrelink's National Support Office can also run these reports.

Conclusion

2.12 The implementation of full logging of all accesses to customer data (which provides a comprehensive audit trail) together with the implementation of a system which allows this information to be easily interrogated and monitored, has satisfied the requirements of Recommendation No.3 parts (a) and (b) of the original report (part (c) is discussed in Chapter 3). It has also assisted in addressing the risks which arise from the wide access to data that Centrelink staff require in undertaking their everyday work. More comprehensive audit trails reduce risks such as the unauthorised browsing, extraction or printing of confidential customer data. These issues were the subject of a number of recommendations in the original report (see Appendix 1).

Privacy Awareness

Issues identified in the original audit

2.13 For many years DSS has placed great emphasis on training its staff in protecting customer data and this was acknowledged at the time of the original audit. The establishment of the Privacy Commissioner's Office (1988) and the updating of the Social Security Act (1991) provided the stimulus for increasing the emphasis on Privacy Awareness training throughout the network. As well, the reviews into customer data confidentiality by the ANAO in 1993 (Audit Report No.23 1993-94 *Protection of Confidential Client Information from Unauthorised Disclosure*) and by the House of Representatives Standing Committee on Legal and Constitutional Affairs in 1994 (*Inquiry into the Protection of Confidential Personal and Commercial Information held by the Commonwealth*) have ensured a continued awareness of the need to maintain high standards in the protection of data.

2.14 In the original audit the ANAO considered that some categories of staff were at risk of lacking full appreciation of their data confidentiality obligations. These were those temporary staff who did not attend the normal induction training program and the new staff who did not attend an induction course until some months after joining DSS. This induction training is important for a number of reasons, including the fact that part of the course is devoted to privacy awareness issues. Without this, the ANAO considered that new and temporary staff might be more inclined than experienced staff to 'browse'

records and may not have a comprehensive understanding of their privacy responsibilities.

2.15 The ANAO made a number of recommendations for improving:

- staff training in privacy and confidentiality; and
- training for Privacy Officers and investigators of alleged breaches.

Follow-up audit findings - privacy training for staff

Training and reference materials

2.16 DSS and Centrelink have continued to update and upgrade the training materials available in different formats (print, video and on-line computer-based) and to provide improved training packages. A *Speakers Kit*, to support the Privacy Officers and Regional Office training officers who deliver formal training sessions has also been developed. The Privacy Section provides material for the use of staff, both handouts in the upfront training sessions, and posters for display in the staff areas of offices. The quality of this material has been improved considerably since the original audit. Centrelink is also developing a series of modules for specialist staff such as social workers and Aboriginal and Torres Strait Islander liaison staff.

2.17 The *Privacy Awareness Kit* comprises the *Confidentiality Manual*, the *Breaches of Privacy and Confidentiality Manual*, the *Privacy Manual* and the National Instructions on privacy and confidentiality. Kits are now primarily intended for on-line use and are no longer issued to all staff in hard-copy but staff are informed that there are several print copies in each office.

Types of training provided

2.18 All staff interviewed, even the most recent new starter, had an understanding of Centrelink's policy on confidentiality. All staff have constant reminders and reinforcement through:

- signing the Declaration of Confidentiality after an explanation of its significance;
- displaying default screen messages after a pre-determined period of time when the computer has not been used (that is, similar to a screen saver);
- new and revised National Instructions;

- educational posters displayed around the office; and
- news items (for example, when someone has been prosecuted for a breach of confidentiality).

2.19 Many of the staff interviewed during the audit advised that they also were given more detail through specific training:

- as part of an induction course;
- through an ASO3 Customer Service course; and/or
- a formal Privacy Awareness training session, generally conducted by the Area Privacy Officer.

2.20 During 1997 the Privacy Officers have provided Privacy Awareness sessions for the staff transferring to Centrelink from DEETYA as well as for new staff. Before Centrelink commenced operations on 1 July more than 3,000 DEETYA personnel and new staff had attended courses. Centrelink's Privacy and Freedom of Information (FOI) Section is delivering courses and distributing material aimed at heightening staff awareness of privacy in the one-stop-shop environment.

2.21 However, through interviews with staff the ANAO identified that nine out of the sixteen staff interviewed had not received formal training although some had been employed for many years. We recognise that these were generally temporary staff who had been in and out of the office on a succession of contracts, or staff who had previously worked part-time but were now full-time. These staff had been advised of the availability of computer-based training (CBT).

2.22 However, the ANAO also found that in some Centrelink offices there is reliance on the availability of computer-based training (CBT) and computer reference material to meet their training requirements in this area rather than attendance at formal training courses. Based on Centrelink survey results, the ANAO was informed however that not all staff are completing the CBT courses. Attendance at a live course, with the interactive discussion, is considered by Privacy Officers to be more effective in ensuring staff are fully aware of the importance Centrelink attaches to confidentiality issues.

2.23 New staff are also told that there is an icon on the computer, which can be used to access on-line all the material in the *Privacy Kit*, should staff need it. However, there are 156 other icons on the computer, which the ANAO considers reduces the likelihood of a staff member locating and studying the items in the *Privacy Kit*.

2.24 It is possible that supervisors may have assumed that, because staff have been employed over a considerable time period, formal training in privacy matters is not necessary. The ANAO also recognises that the provision of formal training can be expensive and time consuming. However, given the value placed on formal training of staff by the Privacy Officers, the ANAO considers that it would be in the interests of both Centrelink and the staff for them to attend a formal training session where this is cost effective. The staff could benefit from the reinforcement provided by a well-presented course. Furthermore, in the event of a future breach resulting in prosecution, from Centrelink's viewpoint such training will provide evidence that the staff member concerned did in fact receive instruction regarding their responsibilities in this area. The staff member therefore could not, as has been done successfully in the past, plead ignorance.

2.25 To ensure that all staff continue to have a comprehensive understanding of their privacy responsibilities Centrelink may also need to consider the cost effectiveness of conducting refresher courses for existing staff where:

- there has been significant changes to protection requirements;
- trend analysis of alleged and substantiated breaches indicates significant recurring problems (this is discussed further in Chapter 3); or
- a lengthy period of time has elapsed since a staff member has attended formal privacy awareness training.

Conclusion - privacy training for staff

2.26 DSS and Centrelink have improved privacy training for staff in line with the recommendations in the original audit report. However, the ANAO found that a significant number of the staff interviewed during the audit had not yet received formal training in this area. There was also evidence that not all staff were completing the CBT packages developed for privacy awareness training. This increases the risk that some staff, mainly temporary officers, may breach the strict confidentiality provisions of the Social Security Act through ignorance of their application in specific work situations. Centrelink needs to ensure that all staff members are fully aware of their responsibilities in relation to the confidentiality of customer information.

2.27 Where it is cost effective, Centrelink should take the opportunity to improve attendance at privacy courses where Privacy Officers present practical examples from the workplace and staff are given the opportunity to discuss relevant issues. If this type of formal training is proved to be not cost effective, then Centrelink should explore other appropriate strategies for ensuring that all

staff are fully aware of their responsibilities in this area and take appropriate action.

Recommendation No.1

2.28 The ANAO *recommends* that Centrelink takes further action to provide all officers, including temporary officers, with a sound understanding of their privacy obligations including through the provision of privacy awareness courses shortly after joining Centrelink, with refresher courses at regular intervals, or through other appropriate strategies where the provision of formal courses is not cost effective.

DSS response

2.29 DSS agrees that further action to improve coverage of privacy awareness training to temporary officers and refresher courses at regular intervals for other officers is appropriate. DSS will be working with Centrelink to revise training packages to address the privacy issues concerning the functions of an officer's particular job.

Centrelink response

2.30 Centrelink agrees that further action to improve coverage of privacy awareness training to temporary officers and refresher courses at regular intervals for other officers is appropriate. Centrelink is presently revising training packages to target training to specifically address the privacy issues concerning the functions of an officer's particular job. For example, training packages are being developed for Callcentre staff, Customer Service officers and managers as well as the Basic training package for all new staff. In this way, staff undertaking new jobs will have privacy awareness training specifically addressing their needs. The Basic training package and the training packages for Customer Service Officers and FOI Officers have already been developed and issued. Packages for Callcentre Officers, Specialist Officers (AILO's, Social Workers etc) and for managers will be issued in the next six months.

Follow-up audit findings - training for Privacy Officers and investigators of allegations

2.31 A number of the recommendations of the 1993 report were focused on DSS providing improved guidance and training for Privacy Officers and for

investigators of privacy and confidentiality allegations (Recommendation Nos. 21-25). In practice, it is usually the Privacy Officer within an Area Office who also has responsibility for investigations of allegations. Many of these officers have a background in investigating customer fraud, and therefore, the investigation of allegations of breaches of confidentiality has similarities with their previous work. However, these officers frequently find themselves conducting investigations into the actions of fellow officers rather than members of the public. This means that the Privacy Officers have particular requirements for support in their work.

2.32 DSS and Centrelink have recently provided more resources into supporting these officers through the development of:

- specialised training courses;
- improved materials for conducting training sessions including a *Speakers Kit*; and
- new or revised manuals including a *Privacy and Confidentiality Breaches Investigations Procedures Manual.*

2.33 In the past, training for these officers was purchased from external providers. However, much of the material presented at such courses did not apply to Departmental situations, for example, forensic work. In May 1997 a purpose designed, in-house course, *CSDA Investigations Training for Privacy Officers,* was introduced. Attendees at this course that were interviewed by the ANAO indicated that the course was valuable. After incorporating lessons learned from the first presentation, further courses are planned.

2.34 Privacy Officers, through the courses that they run for staff, are working to change the perception of their role. The presence of a Privacy Officer in a Regional Office can cause unease amongst the staff. Privacy Officers are seeking to overcome this concern. They wish to be seen as providing support to prevent staff making inadvertent breaches either through ignorance or carelessness rather than investigating after the event. Training courses are therefore slanted towards ensuring that staff are well trained and know where to go for guidance.

Conclusion - training for Privacy Officers and investigators

2.35 The ANAO acknowledges the increased support provided to Privacy Officers and investigators of allegations. DSS and Centrelink have adequately addressed the recommendations of the original report relating to this issue (Recommendation Nos. 21-25).

Customers needing enhanced protection

Issues identified in the original audit

2.36 DSS recognised that some of its customers are concerned that the private and sensitive information which they are obliged to disclose in order to qualify for benefits may become public knowledge. These customers include persons:

- fleeing domestic violence, who do not want their new addresses known;
- who do not wish others to know about their assets; and
- with physical disabilities who do not want their condition to be generally known.

2.37 In 1993 DSS had implemented a process to enhance confidentiality for these customers by placing their records on the Protective File System (PFS). This system combined special clerical procedures with full logging of all accesses to the computer records of those on the system (through the Sensitive Client Data System) to deter unauthorised access.

2.38 However, the ANAO considered that there were weaknesses in the system, that there needed to be a more effective and secure approach to dealing with clients needing enhanced protection, and in particular that procedures needed to be tightened and applied uniformly. The ANAO made several recommendations (Recommendation Nos. 30-32) aimed at:

- tightening procedures and ensuring that both customers and staff clearly understood their application;
- minimising the use of protected file records in systems testing; and
- ensuring that printed reports which identified both protected clients and the users who had accessed the clients' records, could not be accessed by unauthorised staff.

Follow-up audit findings

2.39 The introduction of full logging of staff access to customer data has effectively extended to all Centrelink customers the protection that used to be invoked for the few customers on the PFS. As a result, on the introduction of full logging, DSS and Centrelink sought to reduce the number of people receiving enhanced protection. It has been possible to reduce greatly, in consultation with the customers affected, the number of people receiving enhanced protection.

2.40 For those still requiring enhanced protection, DSS and Centrelink have introduced the Deny Access Facility, which is far more secure in its operation than the PFS. The facility only allows four nominated positions to access the record of a customer granted protection under the facility by a Regional Manager. Customers are required to acknowledge that they will conduct all business with Centrelink through the nominated Responsible Officer positions.

2.41 The Deny Access Facility also ensures that these sensitive records are not selected for testing of program changes.

Conclusion

2.42 The ANAO concludes that DSS and Centrelink have met the audit recommendations and enhanced protection for those at risk over and above that recommended in the original audit.

1.

3. Opportunities for further improvement

Despite many positive initiatives, the number of substantiated allegations against staff has not decreased in the last three years. This points to the need for further improvement. In this chapter, the ANAO addresses four areas where Centrelink should seek to reduce risk - proven cases of breaches of confidentiality, pre-employment checks, high-level access to computer data, and the use of production data in testing.

Introduction

3.1 This chapter discusses the ANAO's findings and conclusions in relation to the remaining major areas identified for follow-up:

- the assessment of the risk of unauthorised disclosure of client information through the use of the detailed analysis of cases of alleged and substantiated breaches of confidentiality in order to determine whether data protection initiatives have been effective;
- the completion of pre-employment checks for all new staff;
- monitoring of unrestricted access to customer data by specialist IT staff; and
- the development of a database of disguised customer data for use in testing computer system changes.

3.2 Each of these areas is discussed in separate sections below.

Analysis of allegations and proven cases

Issues identified in the original audit

3.3 The previous audit report recommended that "the Department ensures regular detailed analysis of allegations of, and proven cases of, unauthorised release of client data and the means employed" (Recommendation No. 1). In its response DSS advised that it agreed with the recommendation and was undertaking such analysis. It also advised "the Privacy Allegation System (PAS) has been developed and implemented which further enhances the Department's ability to analyse cases of unauthorised disclosure".

3.4 In order to assess the ability of Centrelink to perform detailed analyses of cases of unauthorised disclosure the ANAO reviewed:

- the information available from the PAS;
- the analyses of PAS data provided to the Security and Privacy Committee; and
- the analysis of data within the Annual Report.

Follow-up audit findings

Privacy Allegations System

3.5 The development of PAS was completed in the first half of 1995. The system operates from each Area Office and enables the communication of data from these offices to a central database in the National Support Office. There are strict security arrangements to protect information recorded on the PAS, including encryption of all data. Access is restricted to the Privacy Officer and the Control Review and Recovery manager in each Area Office, and selected staff from Administrative Law Branch, National Support Office.

3.6 The PAS is used primarily for case recording and reporting. The system contains three main computer screens. These are the details screen, an investigations screen and an outcome screen:

- the details screen provides basic information on the date of receipt of the allegation, the nature of the allegation, and details of the client whose records are involved and the staff member alleged to have breached privacy;
- the investigations screen includes details of the level of the officer being investigated, the office involved, the source of the allegation, the program involved, the use of logging in the investigation, whether the allegation was substantiated and the date of completion; and
- the outcome screen is only used if the allegation is substantiated. It contains information on referral to other areas, for example, personnel, Director of Public Prosecutions, Australian Federal Police, dates of these referrals and of any subsequent disciplinary or legal action. The screen also contains additional information in respect of cases involving soliciting the disclosure of protected information as these may require investigation by the Australian Federal Police.

PAS data analysis

3.7 Each meeting of the Security and Privacy Committee is provided with a quarterly report containing privacy allegation statistics, largely derived from information contained in PAS. The report contains the following details:

- the number of allegations received and finalised and outstanding for each area office, and, in respect of those finalised, the number substantiated or not substantiated;
- the number of allegations referred to third parties for appropriate disciplinary or other action, that is, personnel, the Director of Public Prosecutions (DPP), the Australian Federal Police (AFP) and so on;
- the number and percentage of allegations by type of breach, for example, browsing, soliciting the disclosure of protected information, misdirected mail;
- the number of allegations received and substantiated, categorised by the salary classification level of staff;
- the number of allegations, categorised by source, such as client, staff, member of public;
- the number of finalised cases where ADP logging information was used to assist in proving or disproving the allegation; and
- cases resulting in charges under the Crimes Act or Social Security Act.

3.8 The report also contains some written comments relating to the statistical data, (however, the ANAO noted that the written commentary is largely the same for each quarter rather than providing specific comments relevant to the specific results obtained for that quarter). The Committee also receives an annual report containing aggregated data for the financial year.

3.9 The ANAO found that the reports provided to the Committee are largely statistical tabulations and contain very little in the way of analytical observations. For example:

- there is only minimal trend analysis comparing the figures with data for previous quarters or cumulative data compared with the same quarter in previous years;
- the annual statistics do not provide a comparison with performance in previous years;
- the reports do not highlight those Areas with a high proportion of substantiated allegations or outstanding cases and whether any action has been taken to identify the causes;
- some substantiated allegations occur in circumstances where no person in particular can be held accountable; a proportion of the remaining substantiated cases are referred to third parties, but there is no indication of the action taken in the remainder; and

- although the source of allegations is provided, there is no analysis of the number of substantiated cases by source.

3.10 The lack of analytical observations has a number of implications for those needing to understand the situation. For example, an ANAO examination of the most recent quarterly report (January - March 1997) revealed that:

- the proportion of substantiated cases was significantly higher in some Areas than others (this outcome would appear to warrant some attention from senior managers to determine the necessary remedial action);
- the statistics for referrals to third parties showed that only 28 out of 96 substantiated cases had been referred to third parties for action and there is no explanation of the lack of action in the remaining cases; and
- the report stated that a single case can be referred to a number of third parties. However, in one Area with only three substantiated cases, the report indicated that five cases had been referred to the DPP and six to personnel (these figures would appear to be incorrect or require some explanation within the report).

3.11 The lack of this type of analysis increases the risk that appropriate action needed to reduce the number of allegations of breaches of privacy may not be identified and undertaken.

Further opportunities for improving analysis of data currently collected

3.12 The ANAO undertook its own analysis of the figures contained in the quarterly reports and found that over the past three years there had been a progressive increase not only in the number of allegations received but also in both the number and percentage of substantiated allegations. The ANAO found that the number of allegations had increased from 919 in 1993-94 to 1121 in 1995-96 (graph 1). It was also found that the percentage of substantiated allegations for finalised investigations had risen from 14 per cent in 1993-94 to 28 per cent in the first nine months of 1996-97. This change is illustrated in graph 3.

3.13 Centrelink advised that the rise in the numbers of allegations received, and in the absolute numbers of substantiated allegations is explained by the provision of more effective privacy education of both staff and the general public and therefore, if people are more aware of what constitutes a breach, then more allegations will be received. They also point out that the inclusion, since 1994-95, of mail-out breaches in the statistics gives a higher figure than would otherwise be recorded. (A 'mail-out breach' occurs, for example, when a letter addressed to a customer has been placed in the wrong envelope, and sent to someone else.) The ANAO considers that, without detailed analysis of individual cases, Centrelink cannot be certain that these reasons are valid or provide a full explanation of the causes of the increases.

3.14 In relation to the rise in the proportion of allegations substantiated, Centrelink advised that the increase was due to 'a combination of record access audit trails (the majority of cases involve improper access to electronically stored client records) and quality investigation techniques employed by Area Privacy staff'. Although the increased substantiation rate can indicate improved detection capacity, the ANAO considers that the fact that both allegations and substantiated allegations have not decreased over time is cause for concern and needs continual monitoring, investigation and implementation of appropriate remedial action.

Opportunities to enhance PAS data collected for analysis

3.15 At present PAS does not contain comprehensive information relating to substantiated allegations. The ANAO considers that further details concerning these allegations would enable Centrelink to identify the circumstances in which breaches are likely to occur, to identify potentially high risk areas, and provide an enhanced understanding of identified trends so that appropriate action can be taken in a timely manner.

3.16 The additional information could be entered into the system through one additional screen in PAS and would only be entered in the event of a *substantiated* allegation. The screen could be used to collect information such as the following:

- personal details of offenders, such as age, sex, length of service, employment status (permanent/temporary/part-time);
- circumstances of breach, such as screens accessed, frequency of access, time of day;

- motivation, for example, pressure from family or friends, financial gain, malice; and
- implications of breach, for example, information provided to other parties, risks to safety of customers, financial disclosure/gain.

3.17 This information would generally be available from either personnel records, CRAM reports or investigation interview records. Centralised analysis of this information together with the existing PAS data would assist Centrelink in identifying the characteristics of staff most frequently involved in breaches and the nature of the most common types of breaches. It would also provide the opportunity to discern patterns and trends in respect of unauthorised access and disclosure and therefore inform decisions concerning the implementation or revisions of strategies designed to minimise the risk of breaches of privacy occurring.

3.18 The ANAO's discussions with relevant Centrelink staff strongly indicate that the development of this additional facility would not involve either significant time or expense.

3.19 This would then allow Centrelink to develop strategies and preventive measures addressing those aspects identified as high risk. The types of measures could include special warnings on screens or records known to attract unauthorised attention, targeted monitoring of high risk screens (for example, the screens which display customer addresses) and directing specialised awareness training at those groups of staff with characteristics identified as most likely to result in breaches.

Conclusion - analysis of allegations and proven cases

3.20 The Privacy Allegation System is used primarily for recording and reporting. However, the reports provided from PAS data to the SPC lack detailed analysis and do not clearly identify overall trends in both the receipt of allegations and the outcome of investigations. The ANAO considers that a more detailed analysis of alleged and substantiated breaches would assist the Committee in making informed decisions concerning the effectiveness of strategies designed to minimise the risk of breaches of privacy.

3.21 The ANAO also considers that Centrelink should examine the viability of enhancing the data collected on substantiated allegations to improve the analysis referred to in the previous paragraph and further inform the work of the SPC.

Recommendation No.2

3.22 In order to provide a basis for measuring the success of, and revising where necessary, strategies implemented with the aim of minimising unauthorised access to, and disclosure of, confidential information, the ANAO *recommends* that Centrelink:

- ensures that information currently collected in relation to alleged and substantiated breaches of privacy is comprehensively analysed;
- undertakes a cost/benefit analysis to determine the feasibility of extending the existing Privacy Allegations System to include further details concerning these allegations in order to identify potentially high risk areas, and provide an enhanced understanding of identified trends so that appropriate action can be taken in a timely manner; and
- ensures that the commentary on the analysis of information collected for the quarterly and annual reports to the Security and Privacy Committee addresses key performance issues, including an analysis of any significant trends identified over longer periods of time.

DSS response

3.23 See Centrelink response.

Centrelink response

3.24 Agreed. Enhancements to the Privacy Allegations Reporting System have already been implemented and further enhancements are planned in the next six months to enable a more comprehensive analysis of statistical data for reporting requirements to the Security and Privacy Committee.

Annual Report

3.25 The ANAO examined the reporting of privacy matters in DSS' Annual reports for the last three years. It was noted that the form of reporting varied for each of these years and it was not possible to make a comparative assessment of DSS' performance based on the material contained in the reports. In some cases the ANAO considers that the material could have been confusing. For example, in one year the figures referred to the number of cases 'received' and the percentage unsubstantiated. In the following year it referred to the number 'investigated' and the percentage unsubstantiated. In neither case did the report indicate the number of outstanding cases. This presentation has been improved in the most recent Annual Report which contains the numbers of cases investigated, substantiated and

unsubstantiated. However, the Report does not contain the number received or the number outstanding at the end of the year. Therefore, the reader can not determine DSS' (Centrelink's) performance in relation to outcomes in this area.

Recommendation No.3

3.26 The ANAO *recommends* that Centrelink develops a consistent format for reporting details of privacy allegations and investigations in its Annual Report that would enable the Parliament and the public to better assess, and discern significant trends in, its performance**.**

DSS response

3.27 See Centrelink response.

Centrelink response

3.28 Agreed. Centrelink has been continuing to improve the recording of statistical data on privacy allegations and will publish comprehensive statistical data to discern significant trends in performance.

Staff recruitment - pre-employment issues

Issues identified in the original audit

3.29 In 1993 the ANAO found that it was DSS policy to conduct pre-employment checks for only some temporary and permanent appointments. In some Areas there were no checks for temporary staff. The ANAO recommended pre-employment checks on all temporary staff who were to have access to confidential client data (Recommendation No.15). The purpose of these pre-employment checks is to assist DSS in determining whether the person to be employed meets the 'fit and proper person' requirement contained in DSS' policy relating to the employment of staff.

3.30 The audit also found that while some temporary staff took part in the normal induction training program, others did not; it seemed unlikely that the 'culture of privacy awareness' could be as effective in the case of temporary staff. The recommendation (Recommendation No.16) was that DSS ensure that temporary staff have sufficient awareness of data confidentiality procedures and practices.

3.31 DSS agreed to make a decision about guidelines on pre-employment checks for all prospective staff. The Department also outlined the privacy awareness training already in place and stated that all staff were provided with an explanation of their responsibilities when they sign the "Declaration of Confidentiality".

3.32 As training issues have been discussed already in Chapter 2, the ANAO in examining this issue looked specifically at:

- pre-employment checks; and
- declarations of confidentiality.

Follow-up audit findings

Pre-employment security checks

3.33 In 1994 the DSS Personnel Management Guidelines relating to pre-employment checking of prospective staff were updated to require that:

- a check of police records is to be undertaken for all prospective appointees (including re-appointees), and temporary employees before any employment commitment is made by the Department;
- in respect of prospective appointees or re-appointees, the police records check will be undertaken prior to appointment to the Department; and
- for temporary employees, the check is to be undertaken prior to the engagement of the person.

3.34 The Guidelines also provide for a person to be temporarily employed pending the results of the police records check if the Delegate determines that 'exceptional circumstances exist'. However, any decision made by the Delegate to proceed with temporary employment pending the results of a police records check should be formally documented and the person notified that the employment is pending the outcome of the check.

3.35 The ANAO notes that a revised set of Guidelines has been drafted (March 1997), but not implemented as yet. The new draft Guidelines still include the requirement to conduct pre-employment checks as detailed above.

3.36 Although there is a risk associated with employing staff before a satisfactory police check has been received the ANAO found that, in two of the three DSS Areas visited, it was not unusual for this to occur. Employees are often required to sign a 'release to obtain information' as well as the 'Declaration of Confidentiality' on the day they commence work. In response to

questions concerning the reasons for adopting this practice the ANAO was informed by staff in these Areas that:

- the new staff member would not be required to handle confidential data;
- delays were to be expected when referrals were made to the AFP, the implication being that it was unreasonable for employment to be deferred until clearances were obtained; and
- it was believed that pre-employment checks had already been completed for people included on the list of applicants for employment supplied by the Area Office.

3.37 The ANAO noted that many temporary staff have access to confidential material as part of performing their normal duties (for example, answering customer inquiries and so on) and it may not always be possible to restrict access to the IT system pending the receipt of an appropriate clearance. It was found that the period between signing the release form and receipt of an appropriate check varies among AFP offices, but at least part of this delay was due to the practice in some Centrelink offices of holding some forms to enable a batch of forms to be sent at the same time. In addition, if the clearance form is only actioned after the employee has commenced, it will inevitably take some time for the clearance to be received and during this period the employee may have access to sensitive material.

3.38 The ANAO observed that procedures had been developed in one Centrelink office to ensure that checks were completed prior to employment. Action was taken to obtain release forms in advance of the prospective employment and a quick turnaround was received from the AFP with the result that employees were (generally) fully cleared before they started work.

Declaration of Confidentiality

3.39 The ANAO considers that the Declaration of Confidentiality to be signed by employees on commencing employment, as well as being a legal requirement, is also an essential element in promoting the culture of confidentiality in DSS and Centrelink. Although all employees are given adequate time to read the Declaration and have the opportunity to ask questions the importance of the document is not always explained to them. ANAO examination of a small sample of personnel files revealed that the documentation was not always complete or up-to-date. In one case the Declaration of Confidentiality was missing and in another the Declaration had not been witnessed. Checklists designed to ensure that all appropriate documentation is placed on personnel files are not always being maintained.

Conclusion - pre-employment issues

3.40 The ANAO considers that some offices are not complying fully with the policy and guidelines on pre-employment checks, and that personnel files are not complete thus increasing the risk that people who do not meet the 'fit and proper person' check may be employed by Centrelink for a short period and therefore have access to confidential customer data.

Recommendation No.4

3.41 The ANAO *recommends* that Centrelink takes action to ensure that:

- all Centrelink offices comply with the policy and guidelines in relation to pre-employment checking of prospective staff;
- persons seeking employment with Centrelink are required to sign the release to obtain information in advance of any prospective employment and that requests for checks are referred promptly to the Australian Federal Police; and
- all necessary documentation is checked prior to employment.

DSS and Centrelink response

3.42 Agreed. The Personnel Management Guideline 5/1994, entitled 'Policy and Guidelines on Pre-employment checking of Police Records for all Prospective Staff' establishes the requirement/process for police checks, based on the requirement of section 34 of the Public Service Act 1922. The message about the 'fit and proper person' test will be reinforced through the reissue of PMG 5/1994 in March 1998.

Programmer and privileged access to computer data

Issues identified in the original audit

3.43 The ANAO report addressed a number of aspects of IT systems and management which had significant implications for the effectiveness of DSS' data confidentiality strategy. The ANAO concern was that access to data should be on a need to know basis, and that there should be an ability to detect and monitor this access. The areas of concern included access by application programmers to the production database, and the numbers of staff with privileged FIRECALL access. FIRECALL is a mainframe facility that provides temporary, but virtually unrestricted, access, to resources that would normally be disallowed by the mainframe security package. These matters

have also been the subjects of repeated recommendations in the audits of the DSS' financial statements in recent years.

Follow-up audit findings

Application programmers and production data

3.44 Application programmers may require access to the production database to enable them to test and correct problems. Programmers with this access can create programs to retrieve large numbers of customer records, and to select finely specified types of information as part of testing. However, the access which is necessary for operational needs could also be used for illegal access to specific records, with little risk of detection. The ANAO recommended 'greater audit trailing of types and levels of access and functions used by application programmers on the production database'. The recommendation in this context was not intended primarily to counter the risk of fraud - audit trailing would certainly have a deterrent effect, however any changes made to customer records which resulted in illegal payments could be expected to be detected through accounting checks. The ANAO recommendation was designed to protect customer data from access which breached the confidentiality provisions of the Social Security and Privacy Acts and which might not otherwise be detected.

3.45 The ANAO acknowledges that it may not be cost effective to monitor all access by all programmers. However, one of the standard reports available on the Security Monitor System (SMS) is the *Model 204 Command Line Report.* This report can be used to target monitoring activities by identifying specific groups of programmers against which the report can be run, for example, it could be used to provide a listing of all programmers who had used the 'DISPLAY' or 'EDIT' commands on-line during a weekend. However, the ANAO was advised that this facility was not used to monitor unauthorised access by programming staff.

FIRECALL

3.46 The reduction of access to FIRECALL, has been on the SPC agenda for some time. Since the last audit, DSS and Centrelink have increased the security of FIRECALL by introducing access groups within FIRECALL. 'FIRECALL Group' allows accesses to be made more specific to the tasks of particular groups, rather than granting full access privileges to every FIRECALL user. There are now six FIRECALL groups at Centrelink, reducing, but not eliminating, the number of staff with access to full 'FIRECALL' privileges.

3.47 When authorised users turn FIRECALL on, the time they are connected is logged, and they are required to enter a comment which describes the reason for the access but there is no detailed logging of actions while FIRECALL is enabled. In addition, the usage of the FIRECALL access is not regularly monitored. Another standard report which can be produced on the SMS is *FIRECALL/Dataset Access Logging Report*. As this report will produce output of a manageable size, the ANAO considers that, if produced on a regular basis, it would facilitate monitoring of FIRECALL accesses. However, the ANAO understands that this report is produced only occasionally.

Security management reports

3.48 As part of the Strategic Security Project[4], the sub-project Security Access Management System (SAMS) will restrict programmer access to production data at the dataset level, but there will be no control at individual record or field levels. Another sub-project, the Security Reporting and Monitoring Project, will provide more of the information on security compliance that management needs for informed decision-making.

3.49 The Security Section can run a range of security reports, but does so only on request rather than as part of a regular system of monitoring. The Security Section does not consider that proactively running and analysing these security reports is its responsibility. The ANAO considers that responsibility for scrutinising these reports should be clearly identified, and procedures developed to ensure these reports are examined at regular intervals to ensure that unauthorised accesses by programming staff is more likely to be detected and the risk minimised.

Conclusion - programmer and privileged access to customer data

3.50 Centrelink IT staff, as with other Centrelink staff, need access to client data to execute their normal duties. However, this access should be on a need to know basis and should be monitored regularly to minimise the risk of unauthorised access to this data. DSS and Centrelink have taken action to reduce the number of staff with unrestricted access, however, monitoring of IT staff access to client data is very limited. Without such monitoring, Centrelink faces increased risk of unauthorised accesses occurring undetected. The ANAO considers that the use of reports for targeted monitoring of programmer access and FIRECALL privileges can be significantly increased to improve the security of client data.

---

[4] The Strategic Security Project was endorsed by the SPC in 1993 and is still continuing.

Recommendation No.5

3.51 The ANAO *recommends* that:

- Centrelink investigates the cost-effectiveness of implementing targeted monitoring of programmer access to the production database, as part of the Strategic Security Project; and
- the use of FIRECALL privileges be monitored regularly.

DSS response

3.52 See Centrelink response.

Centrelink response

3.53 Agreed. A review of the cost effectiveness of monitoring access by staff holding high level privileges was initiated in December 1997. It is anticipated that the review will be completed in April 1998.

Data scrambling project

Issues identified in the original audit

3.54 In 1993 the ANAO was concerned that test data was being created by taking a direct copy of client information which was not disguised in any way. The audit report stated:

> *"The vulnerability in using live client data for test purposes is that details for thousands of clients are unnecessarily exposed to programming staff who do not have an operational need to know the client details. These programmers have access to powerful programming functions to interrogate the full database. This access thus represents an inherently far higher risk than operational staff.*

3.55 In agreeing to the ANAO's recommendation to overcome the problem (Recommendation No.36), DSS responded that it was planning the development of a disguised test data base.

3.56 The ANAO examined the developments in DSS and Centrelink to meet this recommendation.

Follow-up audit findings

Procedures for using data in testing

3.57 A response to the first part of the recommendation (develop procedures for the creation, use and deletion of test customer data) is in place, though the written instructions are minimal, and may not give adequate direction. There is, however, no monitoring of the adherence to these instructions, which, given the large number of test environments in use at any given time raises doubts concerning the timely deletion of customer data after a series of tests have been concluded. The conditions for setting up the testing sites which are spread all around Australia for major releases are, however, very strict and staff involved in the testing are reminded of their ongoing confidentiality obligations.

Data scrambling project

3.58 The second part of the recommendation (create a test data base of disguised client information) has not been implemented, though DSS indicated, in its reply to the audit in 1993, that planning had already begun. However, there was no specific funding for the project. The responsible section received a one-page specification from the Privacy and FOI Section in March 1996. Some progress has been made since then in relation to developing a method of disguising name, street address and bank account numbers but at the time of the follow-up audit field work, this was not in operation. The ANAO recognises that there are complexities which prevent some data changes: for example, it was found necessary to keep the suburb name as postcodes are used in some processing; similarly, while the actual account number is changed, the Bank, branch, and account type details may affect the processing and are retained.

3.59 There are further complexities in scrambling test data as a change to data in one application may ripple through all the others, making the creation of an accurate disguised database difficult particularly when incorporating customer histories, for example, a customer may have had several partners recorded on the Income Security Systems, with children joining, and then leaving, the family unit. Additional complexities arise when testing the interactions of particular payments systems.

3.60 In its 1997 update to its reply to the original audit recommendation, (Appendix A Recommendation 36) Centrelink again reported that it was planning the development of a disguised test data base. However, Centrelink subsequently advised that, given the problems encountered in the project, other strategies may need to be used to protect data (for example, blanking out parts of fields) if the Data Scrambling project is found to be prohibitively difficult or expensive. Centrelink is also concerned that data scrambling may affect the quality of testing. Good testing is vital to Centrelink's business, and Centrelink

therefore has reservations about adding any risk, however slight, to the testing stage of new releases.

Conclusion - data scrambling project

3.61 Recommendation 36 has not been fully implemented. Centrelink continues to use current production data, copied to a test database, in testing program changes.

3.62 The ANAO acknowledges the difficulties in developing a disguised data base, but is concerned about the lack of priority given to implementing the earlier recommendation. The delay in starting work on this project, together with the time taken to prepare a limited specification, indicates that the task was not given a high priority. However, in view of the need to safeguard the privacy of information supplied to Centrelink, it is important that substantial effort be directed towards minimising the risk of unauthorised access and disclosure of client information during the course of testing. The ANAO considers that Centrelink should seek expert advice on industry best practice regarding the protection of privacy and security of customer test data with the view to applying this best practice to Centrelink test data-bases.

Recommendation No.6

3.63 The ANAO *recommends* that, in order to comply fully with the legislative requirements of privacy and confidentiality, Centrelink explore alternative strategies for protecting data during testing, including the option of using outside expertise, if the Data Scrambling project is found to be prohibitively difficult or expensive.

DSS response

3.64 See Centrelink response.

Centrelink response

3.65 Agreed. From 26 January 1998 Centrelink has implemented data scrambling for all customer data extracts used during system testing. Data scrambling enhances the protection of customer information against unauthorised access and disclosure thus ensuring full compliance with the legislative requirements of privacy and confidentiality.

Canberra ACT
17 March 1998

P. J. Barrett
Auditor-General

Part Three

Appendices

Appendix 1

Recommendations and responses from Audit Report No. 23 1993-94
Protection of Confidential Client Information from Unauthorised Disclosure

The assessment of the risk of unauthorised disclosure of client information

ANAO Recommendation 1993	DSS Response 1993 [5]	DSS Response 1997	ANAO Assessment 1997 [6]
1.a The ANAO recommends that the Department regularly assess the external demand for confidential DSS client information in terms of both quantity and price, and how this demand is being met.	The Department does not agree with the first part of this recommendation and does not intend to implement it. The Department does not accept the need for the regular assessments proposed by the ANAO as they would not alter the Department's strategies to minimise the extent of unauthorised disclosure of client data. . . . The Department's legal and ethical obligation to protect client data is not affected by changes to the demand for and price of that data. The continuing risk assessment performed by the Department indicates that the main data item . . . individuals and organisations appear to be interested in is the whereabouts of DSS clients, (i.e. client addresses). With the exception of this anecdotal information it is difficult for the Department to quantify and in some way accurately "measure" the extent and exact nature of the source of this demand.	DSS assesses the risk to customer information by analysing proven cases and monitoring attemps by persons or organisations to obtain customer information.	The ANAO notes that only 12 cases of external persons seeking the disclosure of confidential client information were substantiated and referred to the Australian Federal Police in 1995-96. Analysis of these cases should provide Centrelink with an indication of the information envisaged by the ANAO recommendation. (b)

[5] Where the responses have been lengthy they have been abbreviated, but the key elements have been reflected. For full text, see original audit report.
[6] Comments based on: (a) testing; (b) indicative evidence collected in the course of the audit; (c) no testing.

The assessment of the risk of unauthorised disclosure of client information (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
1.b The ANAO recommends that the Department ensures regular detailed analysis of allegations of, and proven cases of, unauthorised release of client data and the means employed.	The Department agrees with the second part of the recommendation, and is now undertaking such analysis. The Department constantly monitors the changing environment to determine the effectiveness of existing controls and areas where additional controls may be required. For proven cases of unauthorised disclosure of information this monitoring takes the form of a detailed analysis of the modus operandi to determine any additional potential exposures for which controls need to be developed and implemented. . . . In addition, the Privacy Allegations System (PAS) has been developed and implemented which further enhances the Department's ability to analyse cases of unauthorised disclosure.	A management information and monitoring system for all privacy allegations has been developed by DSS. The system is called the Privacy Allegation System (PAS) and records details of cases including nature of the allegation and outcomes etc. Statistical Analysis of all allegations is conducted on a quarterly basis and reports provided to the Security and Privacy Committee. Details of proven cases of unauthorised release are also analysed.	Partially implemented but ANAO considers more detailed analysis would be beneficial. See discussion in Chapter 3, follow-up Recommendation Nos. 2 and 3. (a)

The assessment of the risk of unauthorised disclosure of client information (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
2. The ANAO recommends that the Department review the scope for reducing DSS overall vulnerability to data access. There should be special focus on the use of functions which provide access to client addresses especially large number of addresses.	The recommendation and preceding discussion imply that too many staff in the regional offices have access to the client data base and that the functionality of the look up facility should be restricted. . . . Any reduction in the present level of access to the client data base would result in an unacceptable fall in the level of service that could be provided. In addition, . . . would decrease the capacity of staff to confirm they have accessed the correct client record. . . . The Department would rather implement additional controls or enhance existing controls rather than unduly restrict access and screen dumping facilities.	DSS does not agree with the implication made by the ANAO that the number of staff with access to the client data base should be reduced. The present access levels have been set having regard to client service requirements and the need to protect confidential client information. DSS has moved to reduce the vulnerability of the present level of data access by developing a system to log all access to the client data base. The system will enable DSS and Centrelink to more effectively investigate allegations of unauthorised release of data and will provide a major deterrent effect.	Agree that full logging of access to client data has a major deterrent effect. (c)

The assessment of the risk of unauthorised disclosure of client information (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
3. The ANAO recommends that the Department determine the feasibility of logging all, or an increased percentage of, accesses to client data, through a detailed cost/benefit analysis. Such analysis should address among other things: a. the various types and levels of access and functions which should be logged; b. the data structure at the dataset, record and field level, and the resources required to log accesses at these levels; and c. interim measures such as greater use of random audit trails and targeting trailing on high risk groups.	Agreed. However, the Department will look to a more cost effective and practical solution than slavishly logging all accesses. Work is already underway on such a task. The Department currently logs all access to and from online systems plus the online procedures executed by an individual logon ID. This data is currently kept for 15 days. For specific transactions, generally involving variations to client payment details, an audit log is kept for a period of 15 months to assist with the monitoring process associated with security, fraud and privacy issues. Additionally, the Department keeps snapshot data of all of its master files, or their equivalent, for a considerable period. Extensive monitoring reports, showing significant management information, are periodically provided to management indicating access statistics including any potential security and privacy breaches.	On 17 February 1994 DSS implemented a system to log all online transactions against production data.	Full logging has been implemented. See discussion in Chapter 2. Further work required in relation to part c of the recommendation. See discussion in Chapter 3. (a)

The strategic management of confidentiality issues

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
4. The ANAO recommends that the Department develop more specific and measurable objectives and integrated plans in the area of data confidentiality.	The Department considers that the development of more specific and measurable objectives in the area of data confidentiality is difficult and may not be feasible. However, the Department will consider whether this is possible under the auspices of the Security and Privacy Committee. In this area, the Security and Privacy Committee will monitor the effectiveness of its policy through examination of the workplans of areas affected by that policy. This will include an assessment of whether the workplans have fully covered all necessary activities associated with the Committee's deliberations.	The Privacy and Security Sections submit detailed workplans to each meeting of the SPC. These contain details of objectives and strategies etc and ensures that an integrated approach to data confidentiality is maintained throughout DSS-Centrelink.	The ANAO notes the response. Having the SPC look at the workplans increases the potential for an integrated approach, but does not ensure it. The ANAO considers that the SPC should ensure that the plans do contain measurable objectives and the integration of plans. (b)

The strategic management of confidentiality issues (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
5. The ANAO recommends that the Department better inform its staff of the existence, structure, responsibility and accountability of the Privacy and Review Branch, and particularly the Privacy Section.	Agreed.	The Privacy and Review Branch is now called the Administrative Law Branch and details of its existence and functions is contained in organisation charts and internal directories. The Privacy Section prepares a detailed workplan setting out its functions and responsibilities for each meeting of the Security and Privacy Committee. This plan is then sent with the minutes of the Committee to all Area Offices. The Privacy Section also provides a Help Desk Service which is listed in internal directories.	Agree that the minutes of SPC meetings are available to Area Office managers and to Privacy Officers. Periodic advice to all staff concerning the functions of the Branch and availability of the Help Desk could also be considered. (b)
6. The ANAO recommends that the Department finalise a statement of the structure, functions and responsibilities of the Privacy and Review Branch as a priority, including a clear outline of the reporting lines for the Branch and its working relationship with Security, Fraud and Control Division.	Agreed. The Department already has a statement of the structure, functions and responsibilities of the Privacy and Review Branch. However, the Department accepts the statement could be more comprehensive.	See response to Recommendations 4 & 5 of the original report. The Administrative Law Branch is now part of the Compliance , Fraud and Teleservice Division which was formerly the Security, Fraud and Control Division.	Centrelink provided a chart showing the structure of the new Compliance, Fraud & Teleservice Division. The Security Section is in the Review Management and Recovery Branch; the Privacy Section is part of the Administrative Law Branch. The inclusion of the privacy function in the same Division as Security Section should improve the working arrangements between these two areas. (b)

The strategic management of confidentiality issues (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
7. The ANAO recommends that initial consultation with the Privacy Branch be a requirement in major system development projects, and that system development methodology be amended to specify Privacy Branch as a stakeholder in all developments and be included on all system distribution lists.	Agreed. However, consideration of the extent of consultation with the Privacy and Review Branch should be a decision made by the Project Manager. Project Managers in the Department have sufficient training to be able to identify the major stakeholders in projects.	The DSS Project Lifecycle Booklet has a requirement that the Privacy Section be consulted during the initial stages of any major systems development, and be considered as a potential stakeholder in all projects. This is covered in the updated version of the DSS Project Lifecycle and Review Checklists	The ANAO notes the DSS response, and it would expect monitoring under the auspices of the SPC to ensure that the requirements are actually met. (c)

The strategic management of confidentiality issues (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
8. The ANAO recommends that the Department reassess the effectiveness of its risk assessment in terms of widening its breadth and depth, its adaptability to emerging risk, and how effectively it acts upon the risks identified.	The Department periodically, through the operation of the Security and Privacy Committee, reassesses the effectiveness of its risk assessment policy in terms of the breadth and depth of the risk assessment coverage as well as the applicability and effectiveness of recommended controls. The Committee oversees the operation of emerging implementation plans and work programs for the Security and Control and Privacy and Review Branches.	DSS and Centrelink periodically, through the operation of the SPC, reassess the effectiveness of its risk assessment policy. The Strategic Security Project that is underway involved a wide ranging risk assessment taking into consideration the new environment that will exist following network replacement. Some of the limitations of previous risk assessments were because the Department did not consider it cost effective to conduct risk assessments of areas that were subject to major change under network replacement. DSS and Centrelink conduct risk assessments where needed. Examples are: Mobile Computing and Floppy Disk Drives.	The original recommendation was made by the ANAO in relation to the perceived need to broaden one particular risk assessment, that is, the protection of confidential client information from unauthorised disclosure. Centrelink periodically reassesses the effectiveness of its risk assessment policy. However, the ANAO notes that the three current risk assessments relating to access to information do not address the two examples cited in the original report: • the balance between efficiency/client service considerations and the risk associated with the current level and extent of access to clients' personal details; and • the issue of access protection in relation to data transferred to other agencies. The ANAO considers that this recommendation has been partially implemented. (a)

The strategic management of confidentiality issues (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
9. The ANAO recommends that the Department develop an implementation plan for introducing the additional countermeasures required to protect data from the vulnerabilities identified in its own risk assessment study in this area.	Agreed. The Department has developed an implementation plan for the introduction of the controls identified by its recent risk assessment exercise pertaining to the unauthorised disclosure of client address data by Regional Office staff. Implementation of these controls has commenced and will continue over the next 6 months period.	Agreed. The Department has developed an implementation plan for the introduction of the controls which are being implemented progressively.	DSS and Centrelink have taken action in all the areas of vulnerability mentioned by the ANAO in the original audit, that is, recruitment processes, awareness program, operational guidelines and computer system controls. The latter is being addressed on many fronts within the 12 sub-projects of the Strategic Security Project. (b)

The strategic management of confidentiality issues (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
10. The ANAO recommends that the Department develop a central data base listing all other agencies and individuals that have legitimate and authorised access to DSS data.	Agreed. However, to a large extent, the Secretary's instrument under paragraph 1314(1)(b) of the Social Security Act 1991 addresses this matter. Continual review of this instrument also ensures that DSS records all situations in which confidential information is disclosed to other Commonwealth agencies.	The Department revises the Secretary's instrument (issued under para 1314(1)(b) of the Social Security Act 1991) that lists Agencies authorised to receive DSS data on an annual basis. The instrument now specifies full details about how and in what circumstances information may be disclosed. This instrument was issued as a National Instruction and is available on-line to all Departmental staff and will ensure that DSS staff are fully aware of the agencies to which information is released. All other authorised releases of information are specifically authorised on a case by case basis by senior delegated officers in accordance with a disallowable instrument issued by the Minister for Social Security.	Provided the information is updated on a regular basis, the arrangements in place should meet the intention of the recommendation. (c)

The strategic management of confidentiality issues (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
11. The ANAO recommends that the Department evaluate and review its Management Strategy for data confidentiality.	The Department agrees with the purpose of this recommendation. However, it is not considered necessary as the Department, through the operation of the Security and Privacy Committee, continuously evaluates and reviews the effectiveness of management control pertaining to the protection of client data. The Department also has the advantage of this review conducted by the ANAO to provide information with which to review its Management Strategy for data confidentiality. An extensive program has been undertaken during the past 12 months to make management at all levels throughout the organisation aware of their roles and responsibility in the protection of client data. This awareness campaign is ongoing, monitored for effectiveness, and encompasses all Departmental staff.	The SPC regularly evaluates and reviews its management strategies for data confidentiality through review of Privacy and FOI, Security, Infrastructure Services and Application Services workplans.	The original audit report highlighted 'evaluations'. Within that in-depth evaluation, the ANAO would expect Centrelink to cover all data confidentiality issues. (c)

Operational strategy for the protection of client data

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
12. The ANAO recommends that the Department review and finalise the Privacy Section Strategic Plan, having regard to ANAO findings.	Agreed.	The Privacy Section workplan containing details of stategies for privacy and confidentiality compliance measures is submitted to each meeting of the SPC and updated as appropriate.	The ANAO notes there is regular scrutiny of strategies by the SPC, but considers more detailed analysis of substantiated allegations could lead to revised strategies. (b)
13. The ANAO recommends that the Department review the appropriate resourcing and priorities of the Privacy Section in the light of the Section's Strategic Plan, and the issues raised in this audit.	Agreed.	The resources of the Privacy Section were reviewed taking into account priorities identified in the Privacy Section Workplan etc. The priorities of the Privacy Section are identified in the workplan and submitted to each Security and Privacy Committee Meeting.	Resources and priorities are periodically examined by the SPC. (b)
14 The ANAO recommends that the Department reconsider development and approval processes for privacy materials to ensure more timely implementation of privacy initiatives.	Agreed.	The development and approval processes for privacy materials have been streamlined to ensure timely implementation of privacy initiatives. Privacy materials are updated and revised on a regular basis to ensure materials are current. The Privacy Awareness Kit which now contains the Confidentiality Manual, Privacy Breaches Manual and the Privacy Manual is now available on-line to ensure access for all staff and easier and timely updating. The Satellite Network has also been used to inform staff of changes to privacy and confidentiality matters.	DSS and Centrelink have provided a wide range of support material in response to this recommendation. The ANAO considers that this recommendation has been fully implemented. (a)

Operational strategy for the protection of client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
15. The ANAO recommends that the Department conduct immediate pre-employment checks on all temporary staff who are to have access to client confidential data.	Agreed. The Department is considering implementation of a pre-employment check for all prospective staff, including temporary employees. Such pre-employment checks would include a police records check for details of any criminal convictions, and a check of Social Security records for instances of fraud and receipt of benefit that may be affected by employment. Draft guidelines on pre-employment checks have been developed and were recently distributed to interested parties for comment. A final decision will be made on this shortly.	All staff are checked. See PERSCOM 5/1994 issued September 1994.	Personnel instructions have been issued but practice falls short of the guidelines. See discussion in Chapter 3, follow-up Recommendation No.4. (a)

Operational strategy for the protection of client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
16. The ANAO recommends that the Department ensures, through, for example training/instruction aids, that temporary staff have sufficient awareness of data confidentiality procedures and practices.	Agreed. The Department released interactive Computer Based Training (CBT) on this subject to all officers by diskette, on 18 October 1993. The package is available in National Administration via each Divisional Support Unit. The CBT is one of a range of available competency based training tools, with the advantage of being immediately available to all new starters, temporary and permanent, at every level. . . . Confidentiality training is now immediately available to all staff with the use of the video recording of [a Departmental] satellite program. . . For temporary staff, supervisors are responsible to decide which competencies are relevant for temporary staff dealing with client information. These measures are in addition to the explanation of responsibilities provided to all staff when they sign the Declaration of Confidentiality.	A staff training package has been issued to all Area Privacy Officers who conduct regular training sessions and Induction Courses. A video has also been produced on privacy and confidentiality for training sessions. An interactive Computer Based Training (CBT) package is available for self instruction. All new starters including temporary staff undergo privacy and confidentiality training and are required to sign a Declaration of Confidentiality on joining the Department. The Business TV Unit also runs various segments on privacy and confidentiality for staff.	Agreed. DSS and Centrelink have been active in developing a range of training materials. However, some categories of staff are still at risk of missing out on formal Privacy training. See discussion in Chapter 2, follow-up Recommendation No.1. (a)

Operational strategy for the protection of client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
17. The ANAO recommends that the Department automatically place audit trails on at least a sample of high risk staff groups, for example temporary staff.	The Department does not agree with this recommendation as there is a need to first assess the privacy aspects and cost effectiveness of this control. The Department is presently reviewing its internal security clearance requirements for new staff. Part of this process is to ensure that temporary staff are fully aware of their obligations in terms of browsing and unauthorised disclosure of client information. The Department is presently considering a cost effective and practical solution to the need for more historical information on client data access. The logging of access by temporary staff will be considered in this context.	The logging of access by temporary staff to customer data bases is in place.	In view of the introduction of full logging, Centrelink now can examine audit trails for all staff. The original recommendation has been fully implemented. (a)
18. The ANAO recommends that the Department ensure that briefing for new staff unable to immediately attend induction courses is formal. It should ensure that staff fully understand procedures for data protection of client data.	Agreed. See response to Recommendation 16.	Refer to 16. Briefing for new recruits is individualised and formal. All staff and contractors sign a declaration of confidentiality and are required to be aware of legislative provisions on privacy and confidentiality. The Recruitment Officer reiterates the need for new employees to read and understand procedures for protection of client data while they are with and after they cease employment with the Department.	Refer to 16 above. (a)

Operational strategy for the protection of client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
19. The ANAO recommends that the Department review the organisational placement of, and responsibility for, Privacy/FOI Officers.	Agreed. This will be considered in the context of the development of the Area Staffing Model.	The Area Staffing Model (ASM) allocates an overall dollar amount to an Area Office. Area Managers have been given the responsibility to allocate resources and functions as best meets their operational requirements. The Privacy/FOI functions are placed in the organisation of the Area Office at the discretion of the Area Manager according to those requirements.	Area managers determine the placement of the privacy function having regard to local circumstances. The function is generally located in the Control Review and Recovery area but it has also been placed in the Program area to give it more attention from a policy perspective. The ANAO considers that the intent of the recommendation has been fully implemented. (a)
20. The ANAO recommends that the Department ensure that all duty statements/job descriptions are updated to reflect the duties being undertaken by officers in regards to privacy/confidentiality.	Agreed.	The Department has provision for the generic duty to be included in appropriate officers duty statements. Generic Duty Statement No. 00196 states: "Perform the above in accordance with....; and privacy and security policies".	The DSS response meets the intent of the recommendation. (b)

Operational strategy for the protection of client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
21. The ANAO recommends that the Department provide improved guidance for Privacy/FOI Officers on performance of their privacy functions and related responsibilities.	Agreed.	The Privacy Section has produced a Privacy Manual that specifies the role and responsibilities of Area Privacy Officers. There is also a Privacy and Confidentiality Breaches Investigations Procedures Manual for the use of Privacy Investigation Staff that specifies their role and responsibilities.	The ANAO considers that this recommendation has been implemented in full. (a)
22. The ANAO recommends that the Department provide competency based training and development to Privacy Officers relating to Privacy and confidentiality.	Agreed. There is a current range of national training material already available relating to privacy and data confidentiality that would be of relevance to Privacy Officers. Training Branch will examine the need for the development of specific modules for Privacy Officers with the Privacy and Review Branch.	In 1995 the Department moved away from formalised competency based training. Privacy Officers attend external training courses conducted by the Attorney-Generals Department and specific Universities courses to cover the theory and legislative provisions relating to privacy and confidentiality. The Department has commenced internal training courses for Privacy Investigations to cover practices and procedures. Privacy Officers also attend annual conferences with expert guest speakers to keep them informed of current developments in privacy.	The ANAO considers that the amended form of training satisfies the intent of the recommendation. (a)

Operational strategy for the protection of client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
23. The ANAO recommends that the Department implement standard speakers kit as soon as possible.	Agreed.	A Privacy Speakers Kit has been issued to all Privacy Officers with an accompanying video.	The ANAO considers that this recommendation has been implemented in full. (a)
24. The ANAO recommends that the Department issue appropriate guidance material relating to the investigation process, addressing in particular the issues raised at 4.55 to 4.60 of the report, and ensure compliance with the guidelines.	Agreed. A National Instruction drawing together all relevant material and emphasising the importance of following the procedures was issued on 22 October 1993.	The Privacy Section has issued a Breaches of Privacy Manual available to all staff which outlines how a privacy investigation will be conducted and the rights of staff members under investigation. A Privacy and Confidentiality Breaches Investigations Procedures Manual has also been issued to all Privacy Investigations Officers to guide and inform them about the privacy investigation processes.	The ANAO considers that this recommendation has been implemented in full. (a)
25. The ANAO recommends that the Department provide competency-based training and development to investigators of privacy and confidentiality allegations.	Agreed.	Refer to 22.	Refer to 22. (a)

Operational strategy for the protection of client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
26. The ANAO recommends that the Department review the 28 days standard for completion of investigations, and consider the need for tighter control to prevent investigations becoming excessively lengthy.	Agreed.	The Department has adopted the standard set by the Privacy Commissioners Office of 30 days (60 for review). The Privacy Allegation System (PAS) provides management information on timeliness of investigations.	Material supplied by Centrelink refers to a departmental standard of 60 days from the receipt of the allegation to the submission of the investigative report. (b)
27. The ANAO recommends that the Department ensure that reporting guidelines be reinforced and include provision for progress reporting by central investigation units to the Areas referring cases to them.	Agreed. Refer to comments for Recommendation 24.	The Privacy Allegation System was introduced to monitor Privacy and Confidentiality Investigations.	The ANAO considers that the intent of this recommendation has been fully implemented. However, progress reporting back from central is not an issue in 1997. (a)

Operational strategy for the protection of client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
28. The ANAO recommends that the Department ensure that Area Offices maintain a register of investigations referred to external agencies.	Agreed.	The Privacy Allegation System has provisions for recording referral of matters to the AFP.	The ANAO considers that the intent of this recommendation has been fully implemented. (a)
29. The ANAO recommends that the Department introduce Quality Assurance procedures for investigation of data confidentiality allegations.	Agreed.	The Department has introduced a Privacy and Confidentiality Breaches Investigations Procedures Manual to ensure all allegations of breaches of privacy and confidentiality are investigated in a professional and proper manner. Area Managers monitor the quality of investigations and are required to make decisions on investigation reports prepared by Privacy Investigations Officers.	The ANAO agrees that DSS and Centrelink have improved training in procedures for investigations, in which Area Managers have a clearly defined role. The recommendation is still only partially implemented, in that Quality Assurance processes would be expected to have a national perspective, including comparisons between Areas. (b)

Operational strategy for the protection of client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
30. The ANAO recommends that the Department review arrangements and procedures for the Protective File System to ensure that these client records are protected effectively. In particular, the Department should address the need to ensure uniform application of procedures, and clients' understanding of the protection available.	Agreed. The Department accepts that the communication of the Protective File procedures needs improvement and has already developed and released a revised instruction to staff covering all clients provided with enhanced protection under the Protective File System, including clients under threat of violence. Procedures for dealing with these clients are currently undergoing major review.	A new Deny Access Facility has been introduced to provide additional protection for records where customers are fleeing domestic/physical violence or are in life threatening situations. The Facility only allows four nominated positions to access the record of a customer granted protection under the facility by a Regional Manager. Customers are required to acknowledge that they will conduct all business with the department through the nominated Responsible Officer positions.	The new procedures that have been implemented provide enhanced protection. The ANAO considers that the recommendation has been fully implemented. See discussion in Chapter 2. (a)

Operational strategy for the protection of client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
31. The ANAO recommends that the Department amend its procedures for testing to minimise the use of protected files records in testing.	Agreed. The Department will be considering whether protected files should be excluded from other areas of testing as a part of the review of the Protective File System.	Refer to 30.	Not tested. However, the ANAO considers that the Deny Access Facility would appear to meet the requirements. (c)
32. The ANAO recommends that the Department change the process for printing protected client review reports to avoid delays in printing locally, and ensures regular timely review of accesses.	Agreed. These matters will be dealt with in the context of the review of the Protective File System.	Refer to 30.	The Deny Access Facility meets the intent of this recommendations. (a)

Information Technology (IT) systems and controls over client data

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
33. The ANAO recommends that the Department review existing business practices to address risks associated with screen-dumping of in particular the look-up screen, and that audit trails be considered to monitor use of this facility.	Agreed. The Department will examine the risks associated with screen dumping with a view to tightening controls. However, the Department considers the screen dumping facility is an important part of the operational environment and necessary to maintain an acceptable level of service delivery.	This recommendation has been implemented. Access to IL/IN screens are now logged.	The ANAO considers that the recommendation has been partially implemented. While the ANAO agrees that all screens are now logged, Centrelink is not addressing the second part of the recommendation, which is to monitor their use. Targeted monitoring of access to the IL/IN screens should be one of the factors highlighted in the statistical analysis of PAS data. See discussion in chapter 3. (a)
34. The ANAO recommends that the Department tighten procedures to control the use of data downloading, restricting it to those staff with a definite need, and that the use of that facility be automatically monitored through audit trailing.	Agreed. However, the Department is fully aware of the potential exposure that PCs offer in terms of their ability to download bulk client data to a floppy drive. . . . this particular exposure . . . requiring detailed examination to determine an appropriate control mechanism. This work is currently being undertaken as part of a risk assessment exercise to determine the controls required in a post network replacement environment.	The Department has strengthened controls through a requirement for requests for downloading to be cleared by SPC on a case by case basis.	Evidence to show that the SPC is taking seriously the risk associated with downloading, and ensuring that inappropriate downloading is not carried out. The ANAO considers that the recommendation has been fully implemented. (a)

Information Technology (IT) systems and controls over client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
35. The ANAO recommends that the Department address the risks associated with the ability to print from portable computers, and take corrective measures as necessary. (Such as disabling the print screen facility where appropriate, and development of audit trailing of this facility.)	Agreed. The recommendation does not provide scope for assessing the need for printing capacity from remote terminals. This should be a part of any risk assessment. . . . Currently remote terminals are not configured to enable them to print data.	Finalised. See Mobile Computing Risk Assessment.	The risk assessment does not specifically refer to the printing capability. However it has assessed the overall risk of mobile computing and this will be reduced after the addition of security components. The ANAO considers that the recommendation has been partially implemented. (a)

Information Technology (IT) systems and controls over client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
36. The ANAO recommends that the Department: a. develop procedures for the creation, use and deletion of test data. Adherence to these procedures should be periodically reviewed to ensure compliance; and b. create a comprehensive test database of disguised client information with, as a minimum, name and address disguised.	Agreed. The Department is planning the development of a disguised test data base. Test data is currently extracted from production data after identification of appropriate records for the particular testing requirements. Use of data is defined by test definitions developed by application staff. All test data is currently backed up with a retention period of one month then deleted. Test data remaining in the Application Sub-system is replaced with new test data prior to each testing exercise. The Department will develop these existing practices into a consolidated set of procedures which highlight the responsibilities of staff with regard to privacy requirements.	Agreed. The Department is planning the development of a disguised test data base. The Department will develop existing practices into a consolidated set of procedures which highlight the responsibilities of staff with regard to privacy requirements.	The ANAO considers that the recommendation has not been implemented. Follow-up recommendation 6. See discussion in chapter 3. (a)

Information Technology (IT) systems and controls over client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
37. The ANAO recommends that the Department implement greater audit trailing of types and levels of access and functions used by application programmers on the production database.	Agreed. The Department has already commenced implementation and through its revised mechanisms for the SAS programmers has developed an access control facility for all Departmental staff including application programmers who submit SAS programs against production files. Access to production data by application programmers following the implementation of this facility, and the provision of test files from a centralised source, will be restricted.	Agreed. The Department has already commenced implementation and through its revised mechanisms for the SAS programmers, has developed an access control facility for all Departmental staff including, application programmers who submit SAS programs against production files. Access to production data by application programmers following the implementation of this facility and the provision of test files from a centralised source, will be restricted.	The reply refers to the Security Access Management System, one of the sub-projects of the Strategic Security Project. This has now been implemented in the Regional Offices, but implementation and training is only now beginning in the National Office where application programmers are located. Another sub-project, the Security Reporting and Monitoring Project will have to be completed before the intent of the recommendation is fully satisfied. See discussion in chapter 3, follow-up Recommendation No.5. (a)

Information Technology (IT) systems and controls over client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
38. The ANAO recommends that the Department review the cost/benefit of wider use of data encryption facilities in the context of the network replacement project.	Agreed. As part of the post network replacement risk assessment exercise the Department will review the cost/benefit for the implementation of data encryption facilities. However this review will be in the context of an option that is likely to cost millions of dollars to control an exposure that to the Department's knowledge, has not resulted in a single unauthorised disclosure over the past decade.	Finalised. A Risk Assessment has been conducted of full data encryption and the Department considers that the cost of full encryption is unwarranted. Full data encryption would involve a large cost including, capital and maintenance. The Department considers that only those parts most at risk need encryption, ie Mobile Computing.	The ANAO considers that the cost appears to be prohibitive and the limited amount of encryption is appropriate. (b)

Information Technology (IT) systems and controls over client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
39. The ANAO recommends that the Department dispose or store old data tapes appropriately.	Agreed.	The tapes are degaussed electronically by Computer Service Centres so that they cannot be read or written to, therefore destroying all information on the tapes. Brambles have been contracted to pick up the tapes and destroy them by incineration.	The actions outlined by DSS and Centrelink clearly meet the intent of the recommendation. (c)
40. The ANAO recommends that the Department ensure that all system development plans address the physical security of all data stores containing client data to minimise the risk of theft.	Agreed. System development plans already address the physical security of data stores.	The Project Plan Template is to include a paragraph on physical security. In addition, the proposed work monitoring project will have physical security of all data stores included in its scope.	We note the response. There should be at least some monitoring to ensure this occurs. There is evidence that there is not consistency in relation to storing confidential reports. Centrelink may need to remind network offices to secure data in accordance with instructions. (b)

Information Technology (IT) systems and controls over client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
41. The ANAO recommends that the Department activate the password history option in order to prevent DSS staff re-using the same passwords, and that it reviews its approach to password use and alternative approaches.	The Department does not agree with the first part of this recommendation. The activation of the password history option would, in the Department's view, create additional exposure as staff would tend to write passwords down in case they forget them. The Department agrees to the second part of the recommendation. As part of the post network replacement risk assessment exercise the Department is reviewing its approach to passwords in general and will implement either a system whereby 'one time' passwords are generated through the use of a smart card or some other form of enhanced user authentication.	The Department does not agree with the first part of this recommendation. The activation of the password history option would, in the Department's view, create additional exposure as staff would tend to write passwords down in case they forgot them, however, due to operational needs, ie Agency/DEETYA comms links, password history (8) has been implemented in the Mainframe & LAN environments. The Department is also progressing towards the implementation of SmartCard for user authentication so as to address the exposures associated with fixed passwords.	Implemented; National Instruction was issued on 9 May 1997. With the creation of the new CSDA environment, the transfer of DEETYA staff to Centrelink, and the need for officers from both departments to access the Integrated Employment System, there has been a need to implement password history for the mainframe environment. The Smart Card project is well advanced and should be trialed early in 1998. (a)

Information Technology (IT) systems and controls over client data (cont'd)

ANAO Recommendation 1993	DSS Response 1993	DSS Response 1997	ANAO Assessment 1997
42. The ANAO recommends that the Department tighten procedures for use and allocation of high level privileges such as FIRECALL.	The Department, through its proposed security access management system, will be able to better control access to high level privileges such as FIRECALL. The use of these facilities currently is restricted to specific technical staff who need to use the facilities because no other practical alternative exists. The usage of FIRECALL facilities is continuously monitored. Access to FIRECALL is reviewed frequently by the technical areas involved and annually by the Security Section. In addition, the format of data retrieval using FIRECALL access is not user friendly. To be able to find a client's address and match it to a particular client is very difficult and would require a detailed knowledge of the record formats and how the model 204 stores them. Staff with FIRECALL access do not generally have this knowledge. These factors significantly reduce the risk of unauthorised release of data using FIRECALL access. To the Department's knowledge, there has not been a single unauthorised release of client data using the FIRECALL access.	The Department, through its Security Access Management System (SAMS) is able to control access to high level privileges such as FIRECALL more effectively. The use of these facilities currently is restricted to specific technical staff who need to use the facilities because no other practical alternative exists. The use of FIRECALL facilities is continuously monitored. Access to FIRECALL is reviewed frequently by the technical areas involved and reported on at SPC meetings. In addition, the format of data retrieval using FIRECALL access is not user friendly. To be able to find a client's address and match it to a particular client is very difficult and would require a detailed knowledge of the record formats and how the model 204 stores them. Staff with FIRECALL access do not generally have this knowledge. These factors significantly reduce the risk of unauthorised release of data using FIRECALL access. To the Departments knowledge, there has not been a single unauthorised release of client data using the FIRECALL access.	The ANAO considers that the recommendation has been partially implemented. See discussion in follow-up Recommendation No.5. (a)