The Auditor-General

Audit Report No.8 1999–2000
Performance Audit

Managing Data Privacy in Centrelink

Centrelink

Australian National Audit Office

ISSN 1036-7632

ISBN 0 644 39114 6

Australian National
Audit Office

Canberra ACT
23 August 1999

Dear Madam President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in Centrelink in accordance with the authority contained in the *Auditor-General Act 1997.* I present this report of this audit, and the accompanying brochure, to the Parliament. The report is titled *Managing Data Privacy in Centrelink*.

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

Yours sincerely

P. J. Barrett
Auditor-General

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

AUDITING FOR AUSTRALIA

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

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

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

Telephone (02) 6203 7505
Fax (02) 6203 7798
Email webmaster@anao.gov.au

ANAO audit reports and information about the ANAO are available at our internet address:

http://www.anao.gov.au

Audit Team

Bill Danaher
Ann Thurley

Contents

Summary and Recommendations

Summary 9
Audit objective, scope and focus 9
Audit criteria 10
Audit conclusion 10
Centrelink response 11
Key Findings 12
Recommendations 16

Audit Findings and Conclusions

1. Background 23
   Introduction 23
   Audit objective, scope and focus 26
   Audit criteria 26
   Audit methodology 26
   Previous reviews 27
   The report 28

2. Privacy planning and guidance materials 29
   Introduction 29
   Planning by the Privacy and FOI Section 29
   Risk analysis 30
   Data privacy guidance materials, procedures and manuals 33
   Privacy awareness 35
   Notification of the purpose for which information is collected 36
   Conclusion 37

3. Information technology aspects of data privacy 39
   Introduction 39
   Information technology framework 39
   Information flows into, within, and out of Centrelink 41
   Data repository management 44
   Security architecture 47
   Audit trails 48
   Conclusion 49

4. Operations in Area Offices, Customer Service Centres and Call Centres 50
   Introduction 50
   Area Privacy Officers 51
   Standards for APO operations 53
   Use of the Customer Records Access Monitoring System (CRAMS) 54
   Dealings with customers 56
   Paper files and security 58
   Privacy training in the Centrelink network 59
   Call centre operations 60
   Recently acquired responsibilities 60
   Conclusion 60

5. Management and performance information 63
Introduction 63
Performance information 63
Targets and standards 67
Reporting 67
Conclusion 69

Appendices
Appendix 1—Abbreviations/Glossary 73
Appendix 2—Information privacy principles 77
Appendix 3—Centrelink data privacy performance information 82

Index 83
Series Titles 84
Better Practice Guides 85

Summary and Recommendations

Summary

1. Centrelink provides a range of services on behalf of a number of other agencies, including: the Departments of Family and Community Services; Education, Training and Youth Affairs; Employment, Workplace Relations and Small Business; and Health and Aged Care. Service level agreements are in place which specifically define Centrelink's responsibilities as an agent for these client organisations.

2. As a service provider, Centrelink collects, stores, uses and disseminates personal information for each of its customers. The *Privacy Act 1988* provides a general framework for the handling of this personal information. The Act includes 11 Information Privacy Principles that set down agency responsibilities in relation to data collection, processing, storage, access, use and disclosure.

3. The *Freedom of Information Act 1982* (FOI), along with the Privacy Act, regulates access to personal information while the *Archives Act 1983* complements the FOI and Privacy Acts. The *Crimes Act 1914* has general secrecy provisions for Commonwealth data and prescribes penalties for unauthorised staff access to any Commonwealth data, including personal information held by Centrelink.

4. There is also relevant specific program legislation such as the *Social Security Act 1991*, *Student and Youth Assistance Act 1973* and *Child Care Payments Act 1997*. These Acts give Centrelink the authority to collect personal information and set directions on management activities related to privacy and confidentiality.

5. Given the Privacy Commissioner's key role in respect of the audit topic, the ANAO consulted the Commission throughout the audit on audit criteria and key issues, including on the final draft report.

Audit objective, scope and focus

6. The objective of this audit was to assess the systems put in place by Centrelink to protect data privacy. The audit reviewed the adequacy of the policies, procedures and the administrative framework associated with data privacy and the computer systems that are used to store and disseminate data. The ANAO also examined compliance with legislative requirements. However, the audit did not include a detailed examination of the protection of data privacy by agencies which receive confidential data from Centrelink or the privacy regimes of the private job providers contracted by the Department of Employment, Workplace Relations and Small Business to provide employment services to eligible jobseekers.

Audit criteria

7. The key criteria used to assess data privacy in Centrelink were the Information Privacy Principles in the *Privacy Act 1988* and other relevant legislation. Against these criteria, the audit examined whether Centrelink has implemented sound policies, procedures and systems relevant to privacy issues.

Audit conclusion

8. The ANAO concluded that Centrelink had established key elements of a sound framework to meet the Information Privacy Principles in the Privacy Act and confidentiality provisions in other legislation. Generally, suitable policies, procedures and systems relevant to privacy issues are also in place. However, Centrelink's framework for the management of data privacy was incomplete in that an assessment of risks to data privacy and planning aimed at minimising these risks had not been undertaken at an organisation wide level. As well, Centrelink's performance information on the actual number of privacy breaches or significant influencing factors was not adequate for performance management or accountability purposes. Consequently, Centrelink's management was unable to be assured of the effectiveness, in practice, of the elements of the framework which had been implemented.

9. It is important for effective strategic risk assessment and management that Centrelink identify potential privacy risks and develop a comprehensive plan to deal adequately with data privacy operations and initiatives. The ANAO also noted that, because of the limited nature of its performance information on the actual number of privacy breaches and the significant influencing factors, Centrelink could not effectively monitor and assess its success in achieving privacy outcomes. The ANAO considers that, as well as assessing the achievement of outcomes, the performance information should also cover inputs and outputs to provide useful measures of efficiency and cost effectiveness both for management and accountability purposes.

10. Elements of the framework which actively promoted the notion of data privacy were:

- a good general awareness of privacy matters by staff;
- availability of comprehensive guidance material; and
- well established processes to investigate breaches of data privacy.

11. The ANAO concluded that the information technology systems supporting data privacy were generally sound, being based on well developed and implemented policies and procedures. Users and systems

staff were well aware of their obligations relating to privacy. The resources invested into the recording and maintenance of data allow Centrelink to track and investigate system-related activity. However, the ANAO had some concerns about the overall effectiveness of intended controls where they did not fully address an associated risk, or where an implemented control needed to be refined or modified to reflect recent organisation changes or business practices. Particular actions Centrelink would be well advised to take, in relation to information technology controls necessary to promote data privacy, are as follows:

- development and implementation of procedures relating to the access to, and distribution of, personal information from secondary data stores; and
- identification and removal of discrepancies between staff access rights granted in the IT security system and the access rights actually required for the positions that these staff currently hold in the organisation.

Centrelink response

12. Centrelink has accepted the findings in the report and is closely examining the recommendations with the view of making further improvements in the protection of customers' privacy. In particular, Centrelink is building a formal, structured risk assessment into all its processes. Centrelink also has introduced a Quality Assurance Framework which promotes and supports risk assessment at the team level and has commenced a top driven strategic assessment of business risks which will form the overarching context for the development of individual risk assessments.

Key Findings

Privacy planning and guidance materials

13. The Privacy and FOI Section prepares operational plans that guide its own work program. The section also undertakes privacy impact assessments that could form an element of a comprehensive risk assessment process. However, these steps are insufficient because, while impact statements are prepared for particular risks, there is no overall assessment of risks to data privacy. Consequently, it is possible that significant risks may not be addressed. The ANAO considers that it is important for Centrelink management to identify all the significant potential risks in relation to data privacy issues. Many of the activities currently undertaken by the Privacy and FOI Section would form part of either the deeper assessment of risks, or of the treatment of particular risks. Monitoring and review of underlying levels of privacy breaches in specific areas would help provide feedback on the identified risks. Cyclical monitoring could be specifically directed to give feedback with respect to particular risks. The outcome of this risk assessment should be provided to individual business areas for incorporation into their normal business planning processes.

14. The ANAO found that Centrelink's privacy guidance information, manuals and advice are of a high standard and the information available to staff is current. Centrelink staff can easily access the guidelines and manuals and, if they have specific questions or need to discuss an issue, obtain assistance from Area Office 'help' desks, privacy officers or the Privacy and FOI Section in the National Office. The ANAO found that the Centrelink staff was well aware of the need for customer privacy.

15. The ANAO considers that the introduction of the life-events service delivery arrangements and the greater integration of data at the information technology level will require the review of notices on Centrelink forms that advise customers of how their data may be used. It may be appropriate for the notices to indicate a range of uses for the information supplied.

Information technology aspects

16. The overall findings for this component of the audit were as follows:

- the IT systems policy and procedural framework had been designed and implemented with appropriate regard to Privacy Act requirements;

- Centrelink staff (including IT personnel) were well aware of their obligations relating to privacy; and
- considerable resources had been invested in the recording and maintenance of data to allow Centrelink to track and investigate system related activity.

17. However, there were identifiable weaknesses where the intended controls did not fully address an associated risk, or where an implemented control needed to be refined or modified to reflect recent organisation changes or business practices. Particular actions Centrelink would be well advised to take, in relation to information technology controls necessary to promote data privacy, are as follows:

- development and implementation of procedures relating to the access to and distribution of personal information from secondary data stores; and
- identification and removal of discrepancies between staff access rights and the requirements for positions.

18. Other areas that need remedial action relate to:

- implementing standards to govern the transfer of data into and out of Centrelink;
- ensuring accountability by programmers for data extraction programs; and
- the overall management and monitoring of data store creation and usage.

Operations in Area Offices, Customer Service Centres and Call Centres

19. Area Privacy Officers (APOs) have a key role in maintaining privacy. It is also important that the investigations of privacy breach allegations undertaken by APOs stand up to legal scrutiny. Therefore, the ANAO considers that there is merit in establishing standard induction and related training requirements for new APOs. Concurrently, work standards should be developed for APO operations.

20. Assurance that customer data privacy is being maintained cannot be gained solely through the conduct of investigations of alleged data privacy breaches. Such investigations can only provide a level of assurance in relation to possible breaches actually reported rather than those breaches which may occur but go unreported. To obtain a sufficient level of assurance on this matter, in addition to investigating allegations received, Centrelink should take a more pro-active role in detecting

privacy breaches, that is, by actively investigating breaches rather than waiting for allegations to be made. Investigations directed at particular identified risk areas would be a cost/effective means of pro-actively identifying privacy breaches. Oversight of such a pro-active program could be managed by the Privacy and FOI Section in the National Office with key elements of the necessary follow-up being carried out by the business areas.

21. The measures used to provide certain customers with additional privacy protection were found to be adequate. However, it was also found that more awareness raising should be provided within Centrelink on the use of customer passwords to improve protection as this simple and effective method could be used more widely than is currently the case.

22. The ANAO found that processes in place in relation to customer 'aggression tags' were inadequate. These tags are necessary to warn staff of the antipathy that some customers have towards staff. However, they are not always regularly reviewed to ensure that they reflect the most up to date situation and this is inconsistent with the Privacy Principles.

23. Paper files, as well as electronic files, contain personal information. The ANAO found that possible staff access to paper files and the inappropriate use of the information contained on those files was not routinely considered in the investigation of privacy allegations nor in the provision of update training for staff in Customer Service Centres (CSCs).

Management and performance information

24. The ANAO found that Centrelink does not have a satisfactory range of performance indicators for data privacy and, therefore, is unable to properly determine its success in achieving privacy outcomes. For example, performance information does not include indicators that enable the measurement of the actual number of privacy breaches by staff. The range of indicators for which information is collected should be appropriately expanded and consideration should be given to pro-actively collecting, monitoring and reviewing information on the underlying rate of privacy breaches. Appropriate targets and standards should be set for all indicators for management and accountability purposes.

25. The ANAO also found that the internal and external reporting on data privacy was inadequate. While the narrow range of indicators for which information is collected contributes to the inadequacy of the reports, consideration should also be given to the various means by which the reports themselves could be made more useful. For example, management reports should include qualitative analyses, the presentation of data in a form that makes it more readily understandable to users and the provision of information on the trend in data privacy breaches over time.

Recommendations

Set out below are the ANAO's recommendations with the Report paragraph reference. The ANAO considers that Centrelink should give priority to Recommendation Nos. 1, 3, 5, 7, 8 and 11.

Recommendation No.1 Para. 2.19

The ANAO recommends that:

(a) An overall risk assessment relating to data privacy issues should be undertaken for Centrelink;

(b) the results of this risk assessment be provided to relevant individual business areas for incorporation into their normal business planning and accountability processes; and

(c) the outcome of the risk assessment should guide the work program of the Privacy and FOI Section and the Area Privacy Officers.

Centrelink's response: Agreed.

Recommendation No.2 Para. 3.14

The ANAO recommends that Centrelink, in consultation with collaborating agencies, develop and implement a suitable privacy standard to govern the transfer of data into, and out of, Centrelink.

Centrelink's response: Agreed.

Recommendation No.3 Para. 3.20

The ANAO recommends that administrative procedures relating to the access and distribution of personal information be reviewed to reduce the risk that private personal data in secondary data stores could be misused or inappropriately disclosed. Centrelink should develop and implement appropriate controls to maintain the privacy of customer data, including mechanisms that ensure:

(a) the actual transmission of data in electronic or physical form is undertaken in such a way that the information is secure while in transit and it is received, first hand, by the intended recipient;

(b) that recipients of data containing personal information are made aware of their responsibilities concerning the confidentiality of the material; and

(c) the probity and appropriateness of access, use, and distribution of information outside of the primary mainframe system are monitored on a risk management basis.

Centrelink's response: Agreed.

Recommendation No.4 Para. 3.34

It is recommended that Centrelink ensure that an appropriate record is kept of all computer code used to access or alter personal customer information so that all such actions can be traced and checked, if necessary.

Centrelink's response: Agreed.

Recommendation No.5 Para. 3.40

It is recommended that Centrelink implement appropriate management, including technical controls, to ensure it can manage and monitor adequately data store creation and usage. Such action is also required to ensure data owners and users are made aware of their responsibilities and can be held suitably accountable.

Centrelink's response: Agreed.

Recommendation No.6 Para. 3.47

The ANAO recommends that the software facility controlling use of, and access to, the mainframe system (ACF2) be reviewed for access discrepancies. Such a review should be conducted as soon as possible after the implementation of the new personnel system and identified discrepancies are corrected. The focus of this review should be to ensure that intended access rights for each agency position concerned are consistent with those actually provided.

Centrelink's response: Agreed.

Recommendation No.7 Para. 4.14

The ANAO recommends that Centrelink develop a standard training program to be undertaken by new Area Privacy Officers which covers induction as well as on-the-job training. This program should include specific instruction in relation to investigation skills, Centrelink's privacy framework and to the presentation of privacy material to staff.

Centrelink's response: Agreed.

Recommendation No.8 Para. 4.28

The ANAO recommends that Centrelink implement pro-active monitoring and review of compliance with data privacy and security policies. The monitoring mechanism should be designed to selectively target possible areas of non-compliance and cover all major corporate systems and data stores on a rotating basis at least once every two years.

Centrelink's response: Agreed.

Recommendation No.9 Para. 4.39

The ANAO recommends that:

(a) when completing an electronic record relating to a customer's personal behaviour, it be made mandatory for Centrelink staff to set a date for this notification to be reviewed; and

(b) management systems be implemented to ensure that these notifications reflect the most up to date situation.

Centrelink's response: Agreed.

Recommendation No.10 Para. 4.46

The ANAO recommends that Centrelink ensures that:

(a) Area Privacy Officers be made fully aware of the need to also consider inappropriate access to paper files in their investigations of privacy allegations; and

(b) Area Privacy Officers include appropriate references to the privacy implications of paper files when providing staff training at Customer Service Centres, emphasising that inappropriate use of information from paper files is just as serious as inappropriate use of information from electronic records.

Centrelink's response: Agreed.

Recommendation No.11 Para. 5.21

The ANAO recommends that Centrelink:

(a) review the performance information for data privacy and develop indicators that provide an effective means of monitoring and assessing data privacy outputs and outcomes and the principal factors that influence the achievement of the desired results; and

(b) set performance standards and targets against each indicator and, where possible, identify suitable comparative benchmarks.

Centrelink's response: Agreed.

Audit Findings and Conclusions

1. Background

This chapter provides the background to the audit. It includes an outline of the legislative basis for the collection of personal data and the role of the Privacy Commissioner in the protection of data privacy. The audit objective, scope, focus, methodology and criteria are also discussed.

Introduction

1.1 Centrelink was established as the Commonwealth Services Delivery Agency, an independent statutory authority, on 1 July 1997. Centrelink provides a range of services on behalf of a number of other agencies, including the Departments of Family and Community Services; Education, Training and Youth Affairs; Employment, Workplace Relations and Small Business; and Health and Aged Care. Service level agreements are in place which specifically define Centrelink's responsibilities as an agent for these client organisations.

1.2 The total program payments administered by Centrelink on behalf of the other agencies exceed $42 billion. At 30 June 1998, Centrelink employed about 24 000 staff. It provides services for about 7.9 million customers storing personal information for each of these customers. In 1997–98 Centrelink received 1091 privacy complaints from customers, the general public and staff members in relation to these customers and the handling of personal information. Appendix 3 has information on the resolution of privacy complaints.

Privacy

1.3 Privacy has a number of aspects: freedom from intrusion on private space; freedom from unjustified or unaccountable surveillance; and maintaining knowledge of, and a measure of control over, the collection, storage, use an disclosure of one's personal information. This last aspect is referred to as 'information privacy' and is supported by legislation in many countries, including Australia.

1.4 As the Privacy Commissioner observed an "*individuals right to privacy for his or her personal information is not absolute. The rights of individuals must be balanced with other public interests and competing claims*". Therefore, the total protection of personal information is not an objective of privacy legislation. For this reason, Australian Commonwealth legislation relating to privacy allows departure from basic information privacy principles when the public interest demands it. Also, the total protection of personal information could disadvantage the people involved. For Centrelink

customers, total data protection would lead to a decrease in the quality of services offered. In the Centrelink environment, staff could take longer to access information and could make incorrect decisions if they were not able to easily access all relevant data.

Legislative basis for the collection and management of data

1.5 A range of legal measures provides protection for personal data collected by Centrelink. Certain legislation establishes the legal framework for the collection, storage and use of data. Other relevant legislation exists which is specific to programs administered by Centrelink.

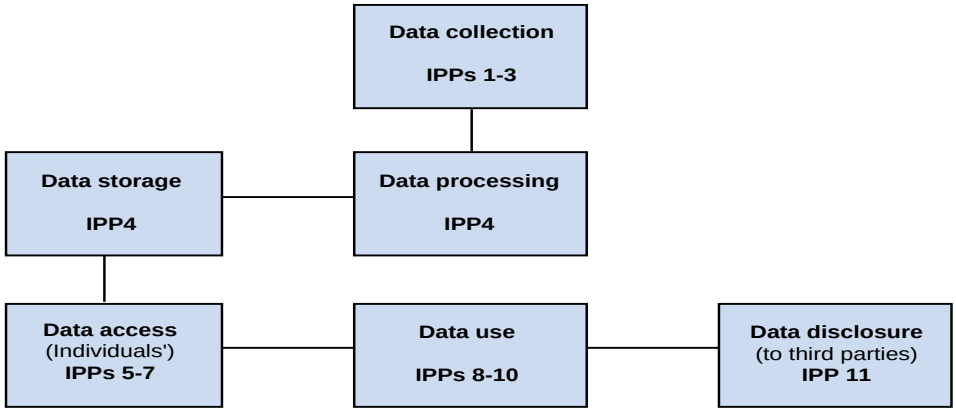
General legislative measures

1.6 A number of legislative measures control the collection, storage, access, use and dissemination of personal information held by Government agencies. The *Freedom of Information Act 1982* (FOI) regulates access to personal information. It allows individuals to access information on themselves and an exemption from protection if the disclosure is in the public interest. The *Archives Act 1983* complements the FOI and *Privacy Act 1988*. It relates to the access to information and considers the reduction in the sensitivity of information with age.

1.7 Complementing the previously mentioned legislation is the *Crimes Act 1914* which has general secrecy provisions for Commonwealth data and prescribes penalties for unauthorised staff access to any Commonwealth data, including personal data.

1.8 The Privacy Act includes 11 Information Privacy Principles (IPPs) which set down agency responsibilities in relation to data collection, processing, storage, access, use and disclosure. The following diagram identifies the stages in the handling of personal information and the relevant IPPs. Appendix 2 provides more detailed information in the IPPs.

Figure 1
Information Privacy Principles



Specific legislation

1.9 Centrelink collects information from customers that is necessary for administrative and accountability purposes. The authority for the data collection and directions on management activities relevant to privacy and confidentiality comes primarily through the *Social Security Act 1991*. Also, there is other relevant legislation for particular client departmental programs such as the *Student and Youth Assistance Act 1973* and *Child Care Payments Act 1997*.

1.10 Personal information collected by Centrelink generally is only for use for the particular purpose for which it was collected. However, the Privacy Act allows for use in a range of other circumstances, set out in the exceptions included in Information Privacy Principle 10. These circumstances include where the customer has consented to another use, use of the information for another purpose is authorised by law and the information is reasonably necessary for protection of the public revenue.

Privacy or confidentiality

1.11 The *Social Security Act 1991*, the *Student and Youth Assistance Act 1973* and other Commonwealth legislation includes confidentiality provisions while the *Privacy Act 1988* has privacy provisions.

1.12 The terms 'privacy' and 'confidentiality' used in these Acts, while similar, are not synonymous. Confidentiality is best seen as a subset of information privacy. Confidentiality deals with limitations on disclosure, that is, who you can tell and under what circumstances. Information privacy deals with those matters, but also with the collection, storage and use of, and with individual access to, personal information.

Role of the Privacy Commissioner

1.13 The role and responsibilities of the Privacy Commissioner are set out in the *Privacy Act 1988*. Among other things, the Privacy Commissioner is empowered to investigate an act or practice of an agency that may breach an Information Privacy principle; examine legislation that may impact on privacy; promote the Information Privacy Principles; and conduct audits of records of personal information maintained by agencies. In resolving a complaint the Privacy Commissioner may seek a settlement when a privacy breach has occurred whereas, with own motion investigations, the Commissioner may seek assurances about the improvement of practices.

1.14 Both the Privacy Commissioner and the Auditor-General are empowered to undertake audits that focus on privacy matters. The Privacy Commissioner is specifically empowered to undertake audits of records of personal information. Consistent with this responsibility, for

example, the Privacy Commissioner has recently completed an audit, within Centrelink, of Newstart Allowance records. In practice, investigations undertaken by the Privacy Commissioner have a slightly narrower focus than those undertaken by the ANAO in that, consistent with the legislation, they relate to "*an act or practice of an agency that may breach an Information Privacy Principle*".

1.15 The ANAO undertakes higher level management reviews and investigates procedures and practices with the aim of determining whether the overall administrative framework of an agency supports the effective and efficient maintenance of data privacy. Accordingly, the work programs of the two organisations complement each other. The ANAO and the Privacy Commission held discussions throughout this audit to develop appropriate audit criteria and key relevant issues.

Audit objective, scope and focus

1.16 The objective of this audit was to assess the systems put in place by Centrelink to protect data privacy. The audit reviewed the adequacy of the policies, procedures and the administrative framework associated with data privacy and the computer systems that are used to store and disseminate data. The ANAO also examined compliance with legislative requirements such as the *Privacy Act 1988*, *Social Security Act 1991*, *Crimes Act 1914* and other relevant Acts.

1.17 The scope of the audit did not include a detailed examination of the protection of data privacy by agencies that receive confidential data from Centrelink. Also, this audit did not consider the privacy regimes of the private job providers contracted by the Department of Employment, Workplace Relations and Small Business to provide employment services to eligible jobseekers.

Audit criteria

1.18 The key criteria used to assess data privacy in Centrelink were the Information Privacy Principles in the *Privacy Act 1988* and relevant legislation. Against these criteria, the audit determined whether Centrelink has implemented sound policies, procedures and systems relevant to privacy issues. Specific details on the criteria used for different issues are found at the start of each chapter.

Audit methodology

1.19 Audit fieldwork was undertaken between November 1998 and March 1999 in Victoria, Queensland and the Australian Capital Territory. Interviews were held with key staff in the National Office in Canberra,

Area Offices, Customer Service Centres and Call Centres. A wide range of documents including guidelines, procedures and training manuals was also reviewed. As well, a consultant was engaged to provide specialist advice on privacy matters while another undertook a review of the information technology systems associated with personal data.

1.20 The audit was conducted in conformance with ANAO auditing standards at a cost of $330 000.

Previous reviews

1.21 Data privacy in Centrelink and, prior to the formation of Centrelink, the Department of Social Security, has been examined previously on a number of occasions. A performance audit by the ANAO on data confidentiality in the Department of Social Security was published in 1993–94. There was also a follow-up to this audit, *Protection of Confidential Client Data from Unauthorised Disclosure* (Auditor-General Report No. 37, 1997–98) which was issued by the ANAO during 1997. This audit has built on the findings of these two audits and tests the adequacy of arrangements put in place by Centrelink to ensure that its customer information is protected. Also, as mentioned above, the Privacy Commissioner has recently completed an audit within Centrelink of Newstart Allowance records.

1.22 Data-matching by Centrelink involves the automated comparison of personal information collected for different purposes and, therefore, has privacy implications. This issue has been addressed previously in two ANAO audits. Data-matching, which was introduced in the 1990–91 Budget, was examined in Audit Report No.7, 1993–94 *Department of Social Security—Data-matching*. That audit found the Department of Social Security had effectively fulfilled its obligations with regard to data privacy. The ANAO undertook a follow-up to this audit, Audit Report No.12, 1996–97 *Data-matching—Department of Social Security*. The follow-up audit did not identify any privacy problems.

1.23 During 1998 there was considerable debate about whether the mail out to pensioners and veterans of information relating to the Community Education and Information Programme (CEIP) was properly made pursuant to the *Social Security Act 1991*. Audit Report No.12, 1998–99 *Taxation Reform – Community Education and Information Programme* addressed this issue. The report indicated that the matter had been referred to the Privacy Commissioner, who was conducting inquiries to ascertain whether the use of pensioner and veteran mailing lists held by Centrelink should be reviewed.

1.24 The then Privacy Commissioner has advised that although she was of the view there has been a breach of the Privacy Act in relation to the use of the pensioner and veterans database, she considered the breaches were minor in nature in that no personal information of the recipients of the mailout was disclosed to any third parties, and their personal information was only used for the purpose of providing them with information. The Commissioner also noted that Centrelink and the Department of Family and Community Services have agreed to implement a number of procedural changes to ensure that there are no similar breaches of the Privacy Act in the future.

The report

1.25 The report discusses findings in relation to the maintenance of data privacy in Centrelink in chapters 2 to 5. Chapter 2 examines privacy planning and guidance materials. Chapter 3 examines information technology related issues while Chapter 4 examines operations in the Area offices, customer service centres and call centres. Chapter 5 addresses management and performance information issues associated with data privacy operations in Centrelink.

2. Privacy planning and guidance materials

This chapter outlines the existing planning arrangements for privacy protection and suggests how these arrangements could be improved. The chapter also examines data privacy guidance materials, procedures and manuals. Guidance materials were found to be readily available and of a high standard. The ANAO also found that the Centrelink staff was well aware of the need for customer privacy.

Introduction

2.1 The ANAO considers it critical that there be a proper risk assessment by Centrelink to identify risks in relation to privacy issues and thus help guide those elements of the agency that have major responsibilities for the maintenance of data privacy. The results of such a risk assessment should also be provided to individual business areas so that their individual plans take account of identified risks.

2.2 Guidelines should exist to assist Centrelink staff to consistently and accurately comply with privacy legislation and regulations and comply with Centrelink policy directions. The guidelines and manuals should be readily available and complete.

Planning by the Privacy and FOI Section

2.3 Central to privacy operations in Centrelink is the Privacy and FOI Section in the National Support Office. The functions of the section are as follows:

- develop policy guidelines and procedures in relation to the privacy and confidentiality of personal information in the possession of Centrelink;
- monitor performance and provide management information in respect of compliance with the Privacy Act and the confidentiality provisions of the Social Security Act, Student and Youth Assistance Act and other Acts administered by Centrelink;
- provide advice and support to all areas of Centrelink on privacy and confidentiality issues. Promote and maintain awareness of these matters throughout Centrelink;
- liaise with the Privacy Commissioner, Attorney-General's and other agencies;

- investigate alleged breaches of privacy and confidentiality; and
- administer lawful disclosures of information

2.4 Planning by the Privacy and FOI Section is structured around these functions but does not include a risk assessment of privacy issues facing Centrelink using a whole of agency approach.

2.5 The principal element of current planning activities is the Work Program Plan. This plan is updated each year with interim reviews if required. The Work Program Plan lists a large number of separate activities that the Privacy and FOI Section undertakes in carrying out its responsibilities. The plan outlines the work needed to be undertaken to develop and maintain guidance material and manuals, monitor privacy allegations, develop training and awareness material and liaise with contacts both within Centrelink and in other agencies such as the Privacy Commissioner and the Attorney-General's Department.

2.6 It is noted that the existing Work Plan is incomplete in that it does not address the last of the functions listed in paragraph 2.3, 'lawful disclosures'. This function should be addressed as processing requests for disclosures of personal information by, for example, the police and Family Law Courts, is a resource intensive responsibility of the section and therefore has a significant impact on the priorities of the section.

2.7 The Security and Privacy Committee (SPC) is a focal point in Centrelink for all security and privacy matters. One of its purposes is to maintain the integrity of security and privacy in Centrelink. The SPC brings its broader perspectives and knowledge to bear on the direction of the Work Plan. However, it is considered that the SPC could more effectively deal with privacy related issues with the benefit of knowledge gained from an assessment of the risks to data privacy undertaken on a whole of agency basis.

2.8 The only risk assessment plan that was drawn to the ANAO's attention was prepared in 1993 and related to aspects of information technology.

Risk analysis

2.9 It is important that Centrelink identifies areas of potential risk in relation to data privacy issues both in the context of Centrelink's strategic and business planning processes and through the work of the Privacy and FOI Section. Otherwise, certain underlying risks may not be addressed. The following discussion refers to those identified by the ANAO. This is not meant to be a stocktake of risks but, rather, illustrative of the approach that Centrelink should pursue.

2.10 There is a risk that, because the Customer Record Access Monitoring System (CRAMS) allows Centrelink staff to comprehensively investigate inappropriate computer access to customer electronic records by Centrelink staff, alternative methods of gaining improper access to information may prove more attractive, for example, paper records. The ANAO found no evidence that privacy officers or CSC managers recognised that paper file records may be more attractive sources of information than electronic files in certain circumstances. Apart from offices where there is off-site storage, there is no record of who might access an individual customer's paper file. Also, there was no evidence put forward in discussions with Area Privacy Officers that access to paper files was considered in the investigation of privacy allegations.

2.11 Centrelink advised the ANAO its long-term strategic goal was to have all paper records stored off-site. A computer program will register the names of all people requesting access to paper records.

2.12 The current use of CRAMS largely relates to confirming or denying allegations that the privacy of particular individuals has been breached in terms of information held electronically. The ANAO considers that there is a risk that privacy breaches are undetected because there is no pro-active monitoring to detect inappropriate staff access to electronic records. Further discussion of how this might be dealt with is found in Chapter 5 of this report.

2.13 The ANAO observed that the move to open planning has associated privacy risks relevant to staff and management. During the past eighteen months, many of the Centrelink CSCs have been physically restructured so that they operate in an open plan environment. The Privacy and FOI Section conducted a privacy impact assessment in respect of the introduction of open plan offices early in this process. The ANAO considers that such involvement is important and benefits Centrelink in that those responsible for implementing such changes need to have independent advice on the privacy risks involved, and how to treat them.

2.14 Particular privacy questions will need to be considered in the future when Centrelink increasingly uses different forms of communications and technology to conduct business with customers and takes on new responsibilities. The ANAO noted that privacy impact assessments were proposed to be fully integrated into the development of a smartcard facility when this was being considered by Centrelink. In regard to other initiatives, the Privacy and FOI Section has had some involvement, although this has been limited in some cases to providing background privacy information.

2.15 While particular business areas are responsible for the implementation of new initiatives, including those aspects related to privacy, the Privacy and FOI Section is responsible for ensuring that privacy risks associated with new initiatives are recognised. That section is involved through its impact assessments or through providing other comments about many of the changes being introduced to Centrelink. The ANAO considers that, while these interventions are beneficial, they tend to be carried out in an ad hoc fashion and not as part of a comprehensive assessment of privacy risks. In addition, the ANAO considers that there are certain underlying risks that may not be addressed by such an approach. For example, in some circumstances new initiatives are interrelated and there may be privacy risks that are not easily identified if the initiatives are examined separately.

2.16 There could also be risks associated with changes to the particular services that Centrelink delivers. In the past eighteen months Centrelink has taken on such matters as service delivery for Youth Allowance and Childcare. Centrelink's role as a service provider may well expand further to undertake the delivery of other services to the Australian community. The Privacy and FOI Section recognises that such new functions contain particular risks and the ANAO considers that its assessment should form part of a comprehensive privacy risk assessment.

2.17 Under the current approach, Centrelink is unable to demonstrate that it is effectively managing the key privacy risks facing the organisation. Given the central role that the Privacy and FOI Section plays in privacy matters in Centrelink, the ANAO considers that the section would greatly assist the organisation by developing a privacy risk assessment on an agency wide basis. Such an assessment would provide a focus for the way in which privacy issues are managed at all levels of the organisation. It would also provide an important input to the SPC and assist it in its efforts to maintain the integrity of privacy in Centrelink. The Privacy and FOI Section could also provide the outcome of its assessment of risks to individual business areas for incorporation in their normal planning processes. Strategies for dealing with privacy risks could include national priorities for area offices and CSCs to pursue.

2.18 Having a comprehensive risk assessment would also operate well in conjunction with the recommendation made in Chapter 5 regarding the monitoring of the underlying level of privacy breaches. The results of the monitoring process could, in certain circumstances, serve to provide feedback to the section in its assessment and treatment of particular risks.

Recommendation No.1

2.19 The ANAO recommends that:

(a) An overall risk assessment relating to data privacy issues should be undertaken for Centrelink;

(b) the results of this risk assessment be provided to relevant individual business areas for incorporation into their normal business planning and accountability processes; and

(c) the outcome of the risk assessment should guide the work program of the Privacy and FOI Section and the Area Privacy Officers.

Centrelink's response:

2.20 Agreed. Various risk assessment processes have been undertaken on different aspects of data privacy and the results used as guides to develop strategies to combat perceived risks eg. the development of targeted training for staff in higher privacy risk areas. Centrelink as an agency has been working towards an overall risk assessment process but this is recognised as a major task given the decentralised nature of its operations and the range of government services provided.

2.21 Centrelink is giving priority to this recommendation.

Data privacy guidance materials, procedures and manuals

2.22 Legislation and good management require the preparation of manuals and guidelines to assist staff to consistently, efficiently and effectively comply with legislation and undertake the administrative functions.

2.23 Centrelink has a range of manuals and guidelines to assist staff in relation to their responsibilities on privacy related matters. The following table provides details of some of the manuals and guidelines available and the staff that they target.

Table 1
Privacy Manuals and guidelines

	Area privacy officers	*Customer Service Centre staff*	*Call Centre staff*	*Centrelink staff—National office*
Privacy awareness kit				
Confidentiality manual	X	X	X	X
Privacy manual	X	X	X	X
Breaches of privacy and confidentiality manual	X	X	X	X
National instructions on privacy and confidentiality matters	X	X	X	X
Other training and guidance materials				
Privacy and confidentiality breaches investigations	X	X involved in investigations		X
Privacy Guidelines				X
Privacy, confidentiality & FOI Centrelink training package	X new starters	X new starters	X new starters	X new starters
Privacy, confidentiality & FOI Centrelink training package (Call centre module)			X	

2.24 As part of its overall training approach, Centrelink also has a Manager's Module that specifically addresses the privacy responsibilities of Centrelink managers. A privacy investigation course was also held for APOs about two years ago. This course is currently being refined with a view to conducting it again in the near future.

2.25 In addition to the above training materials, assistance and guidance is available from:

- training videos;
- bulletins, pamphlets and check lists prepared by the Privacy and FOI Section;
- materials prepared by Area offices to assist with staff induction;
- Area office 'help' desks and privacy officers; and
- the Privacy and FOI Section in the National Office.

2.26 'Screen savers', containing particular privacy messages, are also used to reinforce privacy awareness with staff.

2.27 The ANAO considers that guidance information and advice is readily available. Centrelink staff can easily access the guidelines and manuals from their workstations as it is available on the Centrelink Reference Suite, the major source of text material within Centrelink. If Centrelink staff have a specific question or need to discuss an issue, assistance can be sought from Area Office 'help' desks, privacy officers or the Privacy and FOI Section in the National Office.

2.28 The ANAO considers that guidelines and manuals prepared by Centrelink are comprehensive and of a high standard. Features of the various manuals include:

- background explanations detailing the reasons privacy is important;
- details on the legislative basis for Centrelink privacy policies; and
- the presentation of the IPPs and privacy related legislation in terms and situations familiar to Centrelink staff.

2.29 The information available to staff is current. All of the manuals have been reviewed over the last year and bulletins are prepared to advise staff of current issues.

Privacy awareness

2.30 During the audit the ANAO noted that Centrelink staff were well aware of the need to maintain information confidentiality and safeguard information that may be considered private. This overall regard for the sensitivity of the information retained by Centrelink was observed through:

- the attitude and level of awareness apparent in the staff interviewed during the course of the audit;
- the inclusion of privacy as an integral part of training and induction programs;
- the continual 'presence' maintained regarding privacy and security throughout the work environment through printed material posted on walls and periodic system based reminders; and
- management's establishment of security and privacy control mechanisms as an integral component of most system based activity.

Notification of the purpose for which information is collected

2.31 Information Privacy Principle 2 (IPP2) of the Privacy Act refers to the need for the agency, when collecting information from customers, to ensure that the individual concerned is aware:

- of the purpose for which the information is being collected;
- that the information collection is required or authorised by law; and
- of any usual disclosures of personal information to any person, body or agency.

2.32 The ANAO noted that, consistent with the Privacy Act, forms used by Centrelink for each benefit included an IPP2 notice. Centrelink has recognised that, in the past, the agency did not have a consistent approach to the wording of these notices. On occasions, they could contain too much or too little information. After consultations with the Privacy Commissioner, a framework was developed to guide staff on how the notices should be worded.

2.33 The framework developed for IPP2 notices is suitable for the existing situation. However, changing work practices and technology used by Centrelink could affect the current IPP2 notification used by Centrelink and it may need to be up-dated because, for example, Centrelink is currently developing an alternative service delivery model. The model is based on the life-events that customers may experience rather than the particular payment for which they may be eligible. Customers will be able to approach Centrelink, describe their circumstances and, in return, receive a service offer containing products and services that meet their needs. In this way, Centrelink will deliver to customers service offers tailored to their particular situations. A feature of this model is that each customer will have one main contact in Centrelink with that person taking responsibility for all of the customer's business. This approach to service delivery is currently being trialed in a number of CSCs.

2.34 Changes in the information technology used by Centrelink could also impact on the wording of IPP2 notices. Data for different benefit payment schemes are no longer held in completely separate systems. Data holdings are now considered to be Centrelink data rather than relating to a particular benefit. As is discussed in the next chapter on the information technology systems, a control framework exists to restrict the access of individual officers to particular sets of data. However, customers may need to be advised in the IPP2 notices how the data are held.

2.35 In the light of these developments the ANAO suggests that, when customers first approach Centrelink, consideration be given to advising them, during discussions, that information provided will be used to determine which benefits should be included in the 'service offer' to be made to them, and that over time the same information may be used to reassess their service offer. In addition, given the approach of having one main staff contact for each customer and the pro-active service culture being pursued, it is becoming more difficult to state clearly the purpose for which information is to be used. Accordingly, it is suggested that Centrelink review the form of the words it uses in its IPP2 notices for its various forms. It may be appropriate to indicate a range of uses for the information supplied.

Conclusion

2.36 The Privacy and FOI Section prepares operational plans that guide its own work program. The section also undertakes privacy impact assessments that could form an element of a comprehensive risk assessment process. However, these steps are insufficient because, while impact statements are prepared for particular risks, there is no overall assessment of risks to data privacy. Consequently, it is possible that significant risks may not be addressed. The ANAO considers that it is important for Centrelink management to identify all the significant potential risks in relation to data privacy issues. Many of the activities currently undertaken by the Privacy and FOI Section would form part of either the deeper assessment of risks, or of the treatment of particular risks. Monitoring and review of underlying levels of privacy breaches in specific areas would help provide feedback on the identified risks. Cyclical monitoring could be specifically directed to give feedback with respect to particular risks. The outcome of this risk assessment should be provided to individual business areas for incorporation into their normal business planning processes.

2.37 The ANAO concluded that Centrelink's privacy guidance information, manuals and advice are of a high standard and the information available to staff is current. Centrelink staff can easily access the guidelines and manuals and, if they have specific questions or need to discuss an issue, assistance can be sought from Area Office 'help' desks, privacy officers or the Privacy and FOI Section in the National Office. The ANAO found that the Centrelink staff was well aware of the need for customer privacy.

2.38 The ANAO considers that the introduction of the life-events service delivery arrangements and the greater integration of data at the

information technology level will require the review of notices on Centrelink forms that advise customers of how their data may be used. It may be appropriate for the notices to indicate a range of uses for the information supplied.

3. Information technology aspects of data privacy

This chapter outlines the existing overall IT arrangements for privacy protection including information flows into and out of Centrelink, the storage and use of secondary data stores, access control and audit trails. The chapter has five recommendations relevant to the improvement of these arrangements.

Introduction

3.1 Information technology (IT) systems and hardware are integral to the operations of Centrelink. The Centrelink IT Strategic Plan 1999–2005 states "*A large proportion of the business which Centrelink conducts on behalf of its business clients requires extensive computing support in one or more forms*". IT arrangements to support the protection of customer privacy are an important element of Centrelink's data protection regime.

3.2 The audit examined the information technology infrastructure associated with computer systems that are used to store and disseminate information. The level of breakdowns in the protection of privacy was also examined and the appropriateness of remedial measures assessed. The audit also covered electronic data storage, transfer, and the mechanisms used to protect electronic data from unwarranted browsing, printing and possible sale.

3.3 In the course of its business operations Centrelink provides and receives information from other agencies. However, the scope of the audit was limited to a review of measures in place to provide an assurance that data privacy is being maintained during the transfer process and that the information exchange complies with the Privacy Act requirements.

Information technology framework

3.4 Centrelink's IT hardware infrastructure platform has a number of mainframe processing centres, a Local Area Network (LAN) and a Wide Area Network (WAN). That is, the infrastructure provides servers and personal computers. Also, there is a communications infrastructure which has hubs, routers, and connection to transmission and receiving services. Working on these hardware structures are suites of software that facilitate basic machine operations, coordinate and maintain processing and storage of data, and allow Centrelink staff and clients to access and manipulate data and processing resources.

3.5 To achieve effective, controlled, secure operations and use of IT systems it is necessary to establish an appropriate policy and procedural framework. This framework should articulate the boundaries and standards applicable to an IT system's, data, processing resources and operations. The procedural component of this framework is an integrated set of manuals (that are followed by Centrelink user and systems staff) and automated controls that are enforced or carried out by use of software. These controls are designed to mitigate or negate elements of business or technical risk.

3.6 In order to assess the controls in place in Centrelink regarding privacy principles it was necessary for the ANAO to evaluate the appropriateness and effectiveness of manual and automated controls. The ANAO assessed these controls, primarily, against IPPs 4 and 11 which relate to the storage and security of personal information and limit the disclosure of personal information. Specifically, IPP 4 requires the record-keeper to provide security safeguards to protect the information against loss, unauthorised access, use, modification or disclosure and any other misuse. Also, it requires the record-keeper to protect data privacy when it is passed on to another person in the course of business operations. IPP 11 limits the disclosure of personal information to third parties. More detailed criteria are provided on the following pages for specific issues examined.

3.7 The overall findings of this component of the review were as follows:

- the IT systems policy and procedural framework were adequate, having been designed and implemented with appropriate regard to Privacy Act requirements;
- Centrelink users and systems staff were well aware of their obligations relating to privacy; and
- considerable resources had been invested into the recording and maintenance of data to support the tracking and investigation of system related activity.

3.8 The review also noted some concerns where the intended controls were not fully addressing an associated risk, or where an implemented control needed to be refined or modified to reflect recent organisation changes or business practices. These control deficiencies were not considered to detract from the overall findings of the review relating to privacy, and are discussed below.

Information flows into, within, and out of Centrelink

Modes of information transfer from other agencies

3.9 Data transfers between Centrelink and other agencies should be secure. For this reason, suitable standards for the transfer of data should exist and these should be complied with.

3.10 The Detection and Review (Compliance Services) Branch performs data matching exercises using data from Centrelink and other agencies. Matching exercises assist in the maintenance of information consistency across different government agencies, and in the identification of potential fraudulent behaviour. The *Data-matching Program (Assistance and Tax) Act 1990* and the Privacy Commissioner's Guidelines on Data Matching govern data matching activities in Centrelink.

3.11 It was found that data containing personal information was received by the Compliance Group for matching purposes via:

- computer cartridge and tape;
- SNI link;
- floppy disk through standard mail systems; and
- unsecured internet email.

3.12 While these data transfers are not initiated by Centrelink, unsecured mechanisms for the transfers of data (for example, floppy disks though standard mail systems or unsecured internet email) expose Centrelink (and the provider) to claims that the privacy principles are not being complied with in that insufficient care is being taken to protect data during the transfer process.

3.13 The ANAO considers that Centrelink should address this concern by developing a standard that governs the transfer of data into and out of Centrelink. This standard should address both the format, and transfer, of data.

Recommendation No.2

3.14 The ANAO recommends that Centrelink, in consultation with collaborating agencies, develop and implement a suitable privacy standard to govern the transfer of data into, and out of, Centrelink.

Centrelink's response:

3.15 Agreed.

Access and distribution of information from secondary data stores

3.16 The IPPs require agencies to have measures in place to prevent the unauthorised access, use or disclosure of personal data collected and held by the agency. This requirement extends to secondary data stores as well as primary mainframe systems.

3.17 Within Centrelink, a group of SAS[1] programmers known as the Systems Support Team assists managers to undertake non-routine functions and answer enquiries. Programmers are located in each of the Area offices and they prepare ad hoc management information reports, lists and mailing labels for CSC managers and staff. Regional office staff for day-to-day management and specific purpose mail-outs to Centrelink customers use reports developed by these programmers.

3.18 Several issues were noted in relation to the support function provided by SAS programmers:

- SAS programmers have access to most Centrelink customer information through the Centrelink data warehouse environment. This access is administered by the Knowledge Theme Team and bypasses the Security Access Management System (SAMS) environment (more information on SAMS is provided in paragraphs 3.42 and 3.43). Monitoring of the activities of the SAS programmers is not done within the group, except that all requests are submitted in writing and are registered in each office;
- data extractions which may contain personal information are commonly sent directly to a printer in the requesting CSC or Area Office. If the reports are not taken from the printer immediately the material may be seen or unintentionally collected by someone other than the intended recipient;
- examination of the types of data downloaded to Area Offices or CSCs indicated that personal information could be transferred onto personal computers. This is of concern because once data leaves the mainframe environment standard security arrangements no longer apply. It is considered that Centrelink should assess the security and use of any downloaded data. This assessment should focus on the business reasons for these practices and the level of security being maintained over data still containing personal details; and
- in certain circumstances data or reports extracted using SAS programs are sent out by email. The security requirements for this transfer

[1] SAS (Statistical Analysis System) is a language that is used for routine and ad hoc statistical analyses and quantitative reports.

process should be investigated to ensure that data transmitted this way receives appropriate protection. If necessary, the accompanying email message should make the recipient aware of the security and privacy requirements of the data transmitted.

3.19 The ANAO considers that the processes outlined above could expose Centrelink to criticism because of possible misuse and inappropriate disclosure of private personal data. It is recognised that the analysis of personal data is necessary and greatly assists Centrelink to undertake its business functions. However, the current process controls do not provide sufficient assurance that data security and privacy is being maintained.

Recommendation No.3

3.20 The ANAO recommends that administrative procedures relating to the access and distribution of personal information be reviewed to reduce the risk that private personal data in secondary data stores could be misused or inappropriately disclosed. Centrelink should develop and implement appropriate controls to maintain the privacy of customer data, including mechanisms that ensure:

(a) the actual transmission of data in electronic or physical form is undertaken in such a way that the information is secure while in transit and it is received, first hand, by the intended recipient;

(b) that recipients of data containing personal information are made aware of their responsibilities concerning the confidentiality of the material; and

(c) the probity and appropriateness of access, use, and distribution of information outside of the primary mainframe system are monitored on a risk management basis.

Centrelink's response:

3.21 Agreed.

Ad hoc report release procedures

3.22 The information privacy principles (IPP 4) require record-keepers to do everything reasonably within their power to prevent unauthorised use or disclosure of personal information. This obligation entails the preparation and distribution of procedures on, among other things, the creation and release of ad hoc reports. Procedures should address, among other things, practices necessary to present data in a form that will not allow individuals to be identified.

3.23 Within Centrelink, the Knowledge Theme Team is primarily responsible for the creation and issue of standard reports from aggregated data. In addition to the production of standard reports, the team also responds to ad hoc requests from internal and external sources.

3.24 The ANAO notes that the team is well aware of Centrelink's privacy obligations and possible concerns. However, the specific management and procedures surrounding the creation and release of ad hoc reports are not formally documented. Without clear guidance and procedures addressing the sanitisation, review, authorisation and release of aggregated and detailed Centrelink information, privacy could be compromised. The ANAO considers that documentation relevant to these issues should be updated and that it should provide clear directions on the obligations and standards.

3.25 The ANAO considers that the current procedures surrounding the creation, processing and release of Centrelink information by the Knowledge Theme Team for both standard reporting requirements and ad hoc requests be documented. Centrelink advised the ANAO that the preparation of documentation referred to in this, and the previous paragraph, had commenced.

Data repository management

3.26 The majority of Centrelink's corporate data resides in, and is managed by, Centrelink's 'Model 204' database infrastructure. Within this infrastructure Centrelink's data repository consists of 11 separate databases distributed across five production mainframes located in the Canberra and Sydney data centres. The Model 204 environment supports all online activity and access to client data.

3.27 Business functions within Centrelink, including the Knowledge Theme Team and System Support, require access to the data for aggregation, statistical and ad hoc analysis, and reporting purposes. To minimise the impact on system performance, access to the necessary data is facilitated through strip files. Strip files are extracts of relevant data from the primary data sources. Strip files are created on a regular basis and stored in datasets in the production environment. These files are filtered and sanitised to fulfil specific reporting and analysis needs. This secondary collection of strip files and filtered files can be loosely described as Centrelink's data store.

Access to data repositories by development programmers

3.28 Centrelink retains a team of programmers to support and maintain the applications used to provide services to customers. These

programmers are divided into teams, each supporting at least one service delivery area within Centrelink.

3.29 Centrelink has custom-built information systems which cater for the agency's specific business and information management needs. These systems require periodic maintenance and development to meet the continuing and changing demands of Centrelink's business activities. In addition to these requirements it is necessary on occasions to correct data and processing faults and address data integrity issues.

3.30 A programmer's ability to modify data and run programs in Centrelink's processing environment is controlled by ACF2[2] profiles. When appropriately authorised by the programmer's supervisor, programs are scheduled to run by operations staff.

3.31 As previously indicated (paragraph 3.22), to comply with the information privacy principles, Centrelink must do everything reasonably within its power to prevent unauthorised use or disclosure of personal information. This requirement includes the need for a review process for computer programs that access personal data.

3.32 Those programs that modify or update data for production processing are reviewed by code 'walkthroughs' to ensure that they perform only the functions specified. However, the ANAO considers that this procedure alone does not provide an adequate level of control and exposes Centrelink to the risk that code may be hidden in data extraction programs and that hidden code may be used to obtain data.

3.33 It is recognised that Centrelink IT systems are continually being developed or enhanced and it is not feasible to undertake code reviews for all data extraction programs used in the production environment. However, to address the risk that inappropriate code may be placed in data extraction routines, it is considered that a record should be kept of all code actually run against production datasets. The retention of the actual code run and not allowing this code to be overwritten should deter inappropriate programming practices as it allows an activity to be tracked back to its originator.

Recommendation No. 4

3.34 It is recommended that Centrelink ensure that an appropriate record is kept of all computer code used to access or alter personal customer information so that all such actions can be traced and checked, if necessary.

---

[2] ACF2 is computer software that controls user access to data bases on the mainframe computer.

Centrelink's response:

3.35 Agreed.

Coordination of corporate data management

3.36 It is important in an agency such as Centrelink, which has a large number of primary and secondary data stores, that staff owners and users can be readily identified and be held accountable. A consolidated data use and management directory is necessary to reduce the risk of unauthorised access and unintentional, inappropriate use of data.

3.37 During the course of the audit it was necessary to investigate a number of data management related issues. In the investigation of these issues, it was difficult to ascertain the authority or business group that has the overall responsibility for data management within Centrelink.

3.38 Management of data in the primary data repository is the responsibility of the Data Management Team while an Area group extracting data from the primary data repository is responsible for maintaining the privacy of the data extracted. For example, the Knowledge Team and System Support Group are responsible for the strip files used for statistical and reporting purposes. The audit identified a number of groups creating secondary data stores and, in many instances, such data stores contained private information. However, the ANAO experienced significant difficulties when attempting to identify the group or Area nominally responsible for particular data stores. The ANAO could not identify a consolidated management function that was responsible for the management and tracking of all data use.

3.39 This poses a risk for Centrelink in that, unless the responsibilities for data stores are made clear, staff owners and users of stores may not fully understand or be aware of their specific roles. As a result, there would be an increased risk of unauthorised access and inappropriate use of data. An overall management facility would provide Centrelink with a means of ensuring that owners and users are made aware of their responsibilities and can be held accountable.

Recommendation No.5

3.40 It is recommended that Centrelink implement appropriate management, including technical controls, to ensure it can manage and monitor adequately data store creation and usage. Such action is also required to ensure data owners and users are made aware of their responsibilities and can be held suitably accountable.

Centrelink's response:

3.41 Agreed.

Security architecture

3.42 Consistent with the maintenance of data security, Centrelink is required to have an appropriate security architecture that provides a technical and procedural platform for a security administration process. The aim of the security administration process is to ensure staff access to mainframe applications and data is consistent with their role and position in the organisation.

3.43 Centrelink's security administration relies on a number of IT systems and manual processes. Centrelink's human resource (HR) system, ADMINS, tracks staff members and their occupancy of agency positions. When a new staff member is registered to ADMINS, or a staff member temporarily or permanently moves to another position, ADMINS advises the Security Access Management System (SAMS) of the changes in occupancy. SAMS automatically grants staff the LAN access profiles associated with the position designated in ADMINS. When the responsibilities associated with a given position change and this requires access to different data or system functionality, the position's access profile is altered in SAMS. If changes affect access to mainframe applications, the system sends a message to the mainframe security administrators who update the facility that controls access rights for the particular staff member (ACF2). These updates are normally executed via ADMINS but in certain cases are done directly through the ACF2 native interface. ADMINS is due to be replaced by a new personnel system (SAP HR) by July 1999. A direct link (SAMS Netmaster) is currently being developed and tested to automate ACF2 updates.

Management of staff access rights through the ADMINS/SAMS/ACF2 interface

3.44 Compliance with the privacy principles requires access rights to personal data to be consistent with the duties of a position. The ANAO found that several staff using mainframe applications have more access than appropriate for the positions they occupy. It is considered that under these circumstances there is potential that the privacy of information held on mainframe systems could be compromised.

3.45 Centrelink is aware of this situation as a previous analysis determined that ADMINS-SAMS does not revoke unnecessary elements of a user's access in ACF2 when new access is granted. Cases exist where the old access is retained as well as the new access.

3.46 The security administration area is proposing to rectify this problem with the implementation of the new personnel system (SAP HR) in Centrelink. A new version of SAMS will be released to coincide with

the implementation. This new version aims to interface with the new personnel system in such a way as to ensure that SAMS-ACF2 updates are implemented correctly. At the time of the audit, implementation of the systems in each Centrelink region was expected to occur in late April 1999. However, given that there are Centrelink staff who have access rights which are inconsistent with their current positions, Centrelink will need to review its new systems to be assured that these discrepancies are removed.

Recommendation No.6

3.47 The ANAO recommends that the software facility controlling use of, and access to, the mainframe system (ACF2) be reviewed for access discrepancies. Such a review should be conducted as soon as possible after the implementation of the new personnel system and identified discrepancies are corrected. The focus of this review should be to ensure that intended access rights for each agency position concerned are consistent with those actually provided.

Centrelink's response:

3.48 Agreed. Ongoing management of access is a major focus within Centrelink and a full review of ACF access is nearing completion.

Audit trails

3.49 Central to the maintenance of customer privacy is the need for an audit trail that will allow staff accesses to personal data to be tracked. Audit trails act as a deterrent to illegitimate use and can be used to provide customers with an assurance that electronic records of their personal data have not been improperly accessed. From a Centrelink staff perspective, audit trails are one means of proving that they have not inappropriately accessed data.

3.50 In Centrelink, a consolidated management-audit trail is created using extracts from the mainframe's System Management Facility (SMF) logs and system journal entries from Model 204. The Security Management System (SMS) is the system that maintains this consolidated audit trail. Information in the form of online enquiries and reports is extracted from SMS using the Compliance Reporting Access Monitoring System (CRAMS).

3.51 The monitoring of audit trail information and its use for the creation of performance information is discussed in more detail in Chapter 5 (paragraphs 5.8 to 5.14) of this report.

Conclusion

3.52 The overall conclusions of this component of the audit were as follows:

- the IT systems policy and procedural framework had been designed and implemented with appropriate regard to Privacy Act requirements;
- Centrelink staff (including IT personnel) were well aware of their obligations relating to privacy; and
- considerable resources had been invested into the recording and maintenance of data to allow Centrelink to track and investigate system related activity.

3.53 However, weaknesses were evident where the intended controls did not fully address an associated risk, or where an implemented control needed to be refined or modified to reflect recent organisation changes or business practices. Particular actions Centrelink would be well advised to take in relation to information technology controls necessary to promote data privacy are to:

- develop and implement procedures relating to the access to, and distribution of, personal information from secondary data stores; and
- identify and remove discrepancies between staff access rights and the requirements for particular organisational positions.

3.54 Other areas that need remedial action relate to:

- the development and implementation of a suitable standard to govern the transfer of data into and out of Centrelink;
- continued accountability by programmers for data extraction programs; and
- the overall management and monitoring of data store creation and usage.

4. Operations in Area Offices, Customer Service Centres and Call Centres

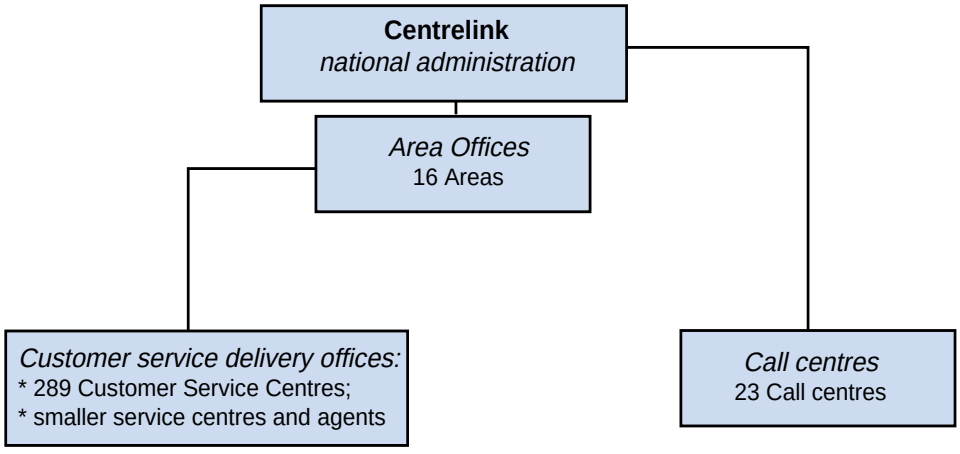
This chapter looks at the protection of data privacy in Area offices, Customer Service Centres and Call Centres. The role and operations of Area Privacy Officers, monitoring of audit trails, interactions with customers, security, training and some emerging issues are discussed. Four recommendations are made in relation to these issues.

Introduction

4.1 Centrelink staff in the Customer Service Centres (CSCs) and Call Centres (CCs) and the Area Privacy Officers play a crucial role in the maintenance of data privacy. CSC and CC staff are the link between the agency and customers. They are provided with personal information by customers, enter it onto computer files, maintain paper records and access both electronic and paper records in the course of normal business. Privacy Officers are located in each Area Office and provide a focus for data privacy operations in the field having advisory, training, investigative and administrative roles. Figure 2 outlines Centrelink's administrative structures.

Figure 2

Administrative structure of Centrelink



4.2 As part of the audit the ANAO visited Area Offices, CSCs and CCs in Victoria and Queensland to assess the efficacy of the network from a data privacy perspective. The ANAO reviewed the operations of Area Privacy Officers to determine if privacy complaints are investigated appropriately and in a timely manner. The ANAO also examined the complaints investigations process to determine if it provides sufficient assurance that customer privacy is being maintained.

4.3 Centrelink should have suitable mechanisms in place to ensure that personal information can only be accessed or released to the person that it relates to or his/her accredited agent. The ANAO assessed these mechanisms for paper and electronic records.

4.4 Some Centrelink customers, such as those who have been in violent relationships, are concerned that the normal arrangements to protect their personal data may not provide them with sufficient protection. The ANAO also examined the arrangements that Centrelink has in place to protect these people to determine if they are adequate.

4.5 Suitable training provides staff with a basic knowledge of privacy laws and regulations. Ongoing training is important because, besides maintaining the currency of staff knowledge, it promotes the development of a privacy culture. The ANAO also assessed these aspects.

Area Privacy Officers

4.6 Area Privacy Officers (APOs) assist staff in Area Offices, CSCs and CCs to protect customers' and staff members' privacy and confidentiality. The APOs provide a helpdesk service; conduct training and outreach visits to CSCs and CCs; facilitate the release of information on privacy; and conduct investigations into allegations of breaches of privacy and confidentiality. The majority of an APO's time is spent on investigations. The APOs report to their local Area Manager, although they have a significant interaction with the Privacy and FOI Section in Gateway Management in the National Office.

4.7 Because APOs play a crucial role in the protection of customer privacy it is important that people with suitable skills are employed and that they have appropriate opportunities to enhance their skills.

4.8 APOs normally have good experience in Centrelink operations prior to taking that position. Based on observations made during visits and discussions with the Privacy and FOI Section, the ANAO concluded that the more effective officers had an aptitude for the work and time to develop their skills in the position. Where officers had been in the job for a relatively short period (less than 12 months), their effectiveness was influenced by the training and induction that they had received.

4.9 The provision of training for recently appointed APOs varied. One relatively new APO, for example, had undertaken little training since moving to this position while another had attended several external training courses on investigation techniques and had also spent time in an adjacent Area Office with experienced staff. It was also noted that in another case a new APO had a substantial handover period and, therefore, the opportunity to learn from his predecessor.

4.10 It is recognised that, while a reasonable handover period is desirable, it cannot always be organised. It was suggested that similar benefits could be obtained if new APOs spent some time in the Privacy and FOI Section in Canberra as part of an induction process.

4.11 Annually, APOs meet in Canberra to discuss privacy issues. In discussions, APOs stated that this conference was a good way to obtain training. In addition, other training opportunities for APOs are provided such as a workshop by an officer from the Director of Public Prosecutions on the requirements for prosecutions. Although the ANAO agrees that such opportunities are an important means of assisting staff to keep across developments in privacy, they do not meet all the training needs of new APOs. In addition, as the conferences are held annually, they may not provide training when new officers require it.

4.12 The arrangements under which new staff were brought into the APO role varied in quality in the Area Offices visited. Given the key role that these officers have in the maintenance of privacy and the need for their investigations to stand up to legal scrutiny, the ANAO considers that there is merit in establishing standard induction and related training requirements for new Centrelink APOs. These programs should be tailored for individual officer's needs and should recognise their prior experience.

4.13 The use of a standard approach to induction and related training, together with work standards discussed below, would provide Centrelink with a sound basis to ensure that APO operations across the network will be effective.

Recommendation No.7

4.14 The ANAO recommends that Centrelink develop a standard training program to be undertaken by new Area Privacy Officers which covers induction as well as on-the-job training. This program should include specific instruction in relation to investigation skills, Centrelink's privacy framework and to the presentation of privacy material to staff.

Centrelink's response:

4.15 Agreed. Centrelink is in the process of evaluating a standard training program for Area Privacy Officers which will meet this recommendation and the requirements of the Commonwealth Law Enforcement Board (CLEB). CLEB requires that all Commonwealth investigating officers be appropriately certified. New Area Privacy Officers will be required to attain suitable qualifications before taking up the duties.

Standards for APO operations

4.16 Given the critical role of Area Privacy Officers in the maintenance of privacy in the network, work standards and targets should be set to promote a consistent and appropriate approach throughout the network. Work standards and targets also provide both Area Management and Gateway Management with a basis for assessing the performance of APOs. The following discussion is on work standards against which APOs can be assessed. Related to the issue of standards for APOs are standards and targets for management and performance information in general—this issue is discussed separately in Chapter 5 of this report.

4.17 The only existing work standard relevant to the operations of APOs is the time taken for the investigation of allegations of breaches of privacy or confidentiality. From the receipt of an allegation 60 days is allowed for investigation and reporting. While the Privacy and FOI Section has prepared guidelines for investigations and reviews a sample of APO investigations, no formal standards for investigations exist.

4.18 The ANAO considers that there is merit in developing other work standards for APOs. Standards could include measures related to both timeliness and quality. Following are some areas where work standards could be developed:

investigations

- minimum satisfactory standard met for investigations as determined by a Privacy and FOI Section review of a sample of investigations; and
- maximum time to respond to the initial complaint and commence the preliminary investigation.

training/outreach

- frequency of refresher courses conducted in CSCs and CCs (annual);
- privacy training for all major groups of new staff including temporary staff; and

- the minimum satisfactory standard for the delivery of training and course material as determined by the Privacy and FOI Section.

4.19 The development of additional work standards should be undertaken in the light of improvements that are made to management and performance information (discussed in Chapter 5). Work standards should be set that are achievable and measurable.

Use of the Customer Records Access Monitoring System (CRAMS)

4.20 Permanent audit trails are essential to protect customer privacy. They act as a deterrent as staff are aware that every access to electronic records is permanently recorded. Also, audit trails may provide basic information needed to investigate allegations of privacy breaches in that they can help clear an accused staff member or provide information essential for preparing a case for prosecution. Therefore, it is important that they exist and are used effectively to identify and deter privacy breaches.

4.21 As mentioned in Chapter 3 (paragraph 3.49), Centrelink creates such an audit trail every time a staff member accesses a customer's personal records by using extracts from the mainframe's System Management Facility logs and system journal entries. CRAMS can be used to generate online reports which show the identity of the person accessing records, access date, time and screen.

4.22 CRAMS reports are generated and used by APOs for privacy allegation investigations if a customer, member of the public, staff or management makes an allegation. These reports are examined to determine if the customer's records were accessed by a specific person and the pattern of access (when and what information was accessed).

4.23 CRAMS, currently, only produces paper reports and these can be voluminous and awkward to use thereby reducing the efficiency of investigations. The ANAO was advised that CRAMS is being enhanced and a screen-based reporting system is being developed to redress this situation. As well, Centrelink is revising the codes used in CRAMS to ensure that they are consistent with those used generally in ISIS.

4.24 The ANAO supports efforts by Centrelink to make CRAMS a more useful and efficient tool for privacy investigations. The improvements to CRAMS as described by Centrelink should make it easier for APOs to undertake routine and pro-active privacy investigations.

4.25 Given the data that Centrelink has available with CRAMS, the ANAO considers that there is substantial scope to make better use of the available information for privacy purposes. The Privacy Act requires

agencies to take reasonable measures to safeguard the confidentiality of information that they store. As there is currently no ongoing mechanism to identify and address inappropriate accesses to private information, Centrelink can not be assured that the protection provided for personal data is adequate. This concern also relates to the comments made in Chapter 5 on the need for improved performance information (paragraph 5.7).

4.26 Centrelink has, however, used CRAMS for a small study in one location that concentrated on staff browsing the records of friends/relatives (ie not in the line of their official duties). The study identified a number of potential breaches of regulations and suggest that statistics produced by Centrelink on the number of proven privacy breaches is significantly less than the actual number of breaches.

4.27 Given this work, the ANAO supports Centrelink taking a more pro-active role in detecting privacy breaches by undertaking similar inquiries on a broader basis rather than waiting for an allegation of a breach to be made by an individual. The ANAO suggests that detection efforts directed at particular identified risk areas would be workable. For example, newly recruited staff or an office which had recorded a substantial number of proven privacy breaches. Oversight of a broader pro-active program could be managed by the Privacy and FOI Section in the National Office with key parts of the checking process being carried out by the business areas. Such an approach would increase the probability that offences could be detected as it would not rely on customers or staff alleging a privacy breach to initiate an investigation. Further discussion related to expanding these efforts to provide performance information is provided in the following chapter (paragraphs 5.8 to 5.14).

Recommendation No.8

4.28 The ANAO recommends that Centrelink implement pro-active monitoring and review of compliance with data privacy and security policies. The monitoring mechanism should be designed to selectively target possible areas of non-compliance and cover all major corporate systems and data stores on a rotating basis at least once every two years.

Centrelink's response:

4.29 Agreed. Centrelink is conducting a pilot study of how to use monitoring reports more efficiently for evaluating compliance with data privacy. The pilot is designed to evaluate different methodologies for monitoring and will determine the cost efficiencies and identify the regularity of any review.

Dealings with customers

4.30 Privacy issues arise in Centrelink's daily dealings with customers. Centrelink has in place a number of mechanisms to provide assurance to customers that privacy is protected.

Customer concern over data privacy

4.31 In certain circumstances it is essential to provide additional protection for the records of Centrelink customers. For example, a privacy breach for a Centrelink customer in an abusive relationship or a witness protection scheme could have serious consequences. Alternatively, a customer could be concerned that a former partner could deceive Centrelink staff on the telephone to obtain personal information.

4.32 In many cases the standard measures taken by Centrelink to address customers' concerns are adequate. Centrelink's first response is to advise the customer of the importance placed by Centrelink on privacy and the overall controls in place. As well, customers are advised that Centrelink can check which staff members have accessed their records. However, Centrelink provides two more levels of protection for customers who need additional protection for their records. These are as follows:

- the "Deny Access" facility for electronic and paper records—this facility limits to a select few the number of staff who are able to access either the electronic or paper file records of the customer; and
- password protection for electronic files—in this situation a customer chooses a password which must be given before information will be released. Without this password, anyone trying to impersonate a customer can not obtain personal details or change the customers records.

4.33 Both of these mechanisms have their strengths and weaknesses in meeting privacy concerns. "Deny Access" is obviously the most secure of these facilities as both electronic and paper files are protected. However, there is a reduction in the timeliness of the provision of services for the customer because he/she must personally visit the specific CSC that retains their records and they have a restricted capacity to use CC facilities. On the other hand, a password provides reasonable security that prevents members of the general public from inappropriately obtaining information. However, it does not prevent inappropriate access to files by Centrelink staff.

4.34 The ANAO found that the Deny Access facility was managed appropriately in the CSCs visited and customers' privacy would be

protected. While the password facility provided the necessary level of protection in the CSCs visited, Centrelink staff knowledge of this facility varied. It is suggested that more publicity within Centrelink be given to the potential benefits of using the password facility in certain circumstances.

4.35 Since April 1999 Centrelink has had a new facility by which customers are provided with a PIN number which can be used to make certain straightforward telephone inquiries in a secure manner. For these inquiries answers are given automatically and there is no Centrelink staff involvement.

Customer aggression

4.36 On occasions some customers display aggressive behaviour when visiting Centrelink offices. As a warning to Centrelink staff a 'tag' may be placed on a customer's electronic records to indicate that an incident has occurred. The Privacy Principles (IPP8) require Centrelink to ensure that personal information is accurate and up to date. In this context, tags associated with particular customers should be reviewed to ensure that they accurately reflect the current situation.

4.37 The ANAO noted that recognition of the need to review these notification tags varied between CSCs visited. It was also noted that it was not mandatory to include a review date when placing a tag on a customer's records.

4.38 To make sure all CSC staff comply with IPP8 the review date on the initial notification should be a mandatory field and managers should be reminded of the need to regularly review this information to ensure that it remains appropriate.

Recommendation No.9

4.39 The ANAO recommends that:

(a) when completing an electronic record relating to a customer's personal behaviour, it be made mandatory for Centrelink staff to set a date for this notification to be reviewed; and

(b) management systems be implemented to ensure that these notifications reflect the most up to date situation.

Centrelink's response:

4.40 Agreed.

Paper files and security

4.41 The Centrelink computer-based income support system, Income Security Integrated System (ISIS), has a large amount of information on customers and Centrelink dealings with these customers. ISIS has increasingly become the main source of information for staff. The trend towards the greater reliance on electronic records will continue.

4.42 Under existing operating arrangements there is a need to maintain some information on paper files as well as maintaining electronic records. Examples of documents that need to be maintained on paper files at this time include the original signed applications from customers, copies of documents used to prove their identity and medical certificates provided by doctors. The filing of papers in most CSCs is done by:

- creating customer files that can contain original applications and copies of certain key documents; or
- batch filing documents, whereby all forms of a particular type lodged on a particular day are stored together.

4.43 The customer files are filed alphabetically and it should be generally straightforward to access a particular customer's file. However, accessing a document for a particular customer that has been batch filed is a complex and time consuming task.

4.44 The ANAO found at the CSCs visited that staff were well aware that paper files should not be able to be read by visiting customers. Staff, therefore, generally turned files down so that they could not be read and complied with the clean desk policy. This approach to the security of information and awareness is very important now that most of the CSCs are operating with an open plan type of fit-out.

4.45 However, another area of information security that should be considered relates to the general storage of the files. The ANAO considers that Centrelink staff were not generally aware of the risk to privacy associated with storing customer files on open shelves in alphabetical order. In addition, in examining details relating to investigations, the ANAO saw no evidence that the APOs considered the possibility of information on paper files being used inappropriately. The ANAO considers that APOs doing risk assessments in the CSCs and investigating allegations of privacy breaches should consider the ease of access to paper files. In the ANAO's view the principal risk with paper files relates to staff inappropriately accessing information on these files. Accordingly, it should be drawn to the attention of staff that the information on paper files should receive the same level of protection as electronic records. Raising this issue in training sessions would increase staff awareness of this risk.

Recommendation No.10

4.46 The ANAO recommends that Centrelink ensures that:

(a) Area Privacy Officers be made fully aware of the need to also consider inappropriate access to paper files in their investigations of privacy allegations; and

(b) Area Privacy Officers include appropriate references to the privacy implications of paper files when providing staff training at Customer Service Centres, emphasising that inappropriate use of information from paper files is just as serious as inappropriate use of information from electronic records.

Centrelink's response:

4.47 Agreed. Centrelink is revising its Privacy Investigation Manual. This issue will be covered in any standard investigation training course for Area Privacy Officers. It will also be taken into account in developments in Record Management.

Privacy training in the Centrelink network

4.48 Privacy training for Centrelink in the network is an important facet of data protection. Privacy training is generally delivered by Area Privacy Officers although some Area Offices have specialist training officers who may also provide some privacy training during the induction of new employees.

4.49 The ANAO found that privacy training availability and standards tended to vary between the CSCs. The standard of the training was a reflection of how confidently APOs dealt with general privacy responsibilities and their experience in delivering training presentations.

4.50 In addition, the ANAO was advised at a particular CSC visited that privacy training was included in a comprehensive training package that had been prepared by a training officer. This training was provided for all new staff, including temporaries.

4.51 The frequency of privacy education programs designed to update staff knowledge and awareness of privacy issues was also variable. Some of the APOs interviewed had a strategy of providing all CSC and CC staff with privacy training each year. Others tended to carry out training in a more random manner. These courses do not need to be lengthy but should refresh staff awareness and bring them up to date on privacy developments.

4.52 Given the importance of the training function for the APO and its contribution towards the maintenance of customer privacy, the ANAO suggests that the standards for Area Privacy Officers that were discussed previously (paragraphs 4.16 to 4.19) should address the quantity and quality of training delivered.

4.53 To help assess the effectiveness of privacy training, the ANAO had discussions with staff in both CSCs and CCs and examined a limited number of paper records at certain CSCs. The ANAO found staff awareness of privacy issues to be generally high. In examining a number of paper files at certain CSCs the objective was to determine whether there was any information on the files that was unnecessary or inappropriate. No inappropriate information or unnecessary comments were found on the files examined. However, the ANAO noted that some tax file numbers had not been removed from documents as required by the Privacy Commissioner's Tax File Number Guidelines. Also, some confidential medical records were not in the envelopes provided for that purpose.

4.54 Centrelink guidelines allow for credit cards to be used as a secondary proof of identity. However, the ANAO noted that at two CSCs visited, photocopies of credit cards had been placed on the customer files that showed the account number and card expiry date. This information could be used by others to obtain goods fraudulently. The ANAO suggests that Centrelink provides additional guidance to staff on the collection and storage of identification material.

4.55 The ANAO considers that update privacy training should address, among other things, local privacy problems. To the extent that particular allegations have been made and proven at particular locations, APOs should make sure that relevant issues are properly covered during training. APOs are already encouraged to invite comment from managers, FOI officers, compliance officers and office trainers before delivering privacy training. The ANAO considers that the relevance of privacy update training could be improved if APOs also undertook preliminary investigations of privacy practices in a particular CSC prior to delivering the training for staff in that location. This could include visiting the office prior to delivering training, observing the general work environment that staff were operating in and examining a sample of paper and electronic records.

4.56 The ANAO suggests that APOs undertake surveys of potential privacy weaknesses in CSCs and CCs before delivering privacy training programs at these Centres.

Call centre operations

4.57 The ANAO visited two call centres during the audit and spoke to staff, observed privacy checks undertaken by staff and had general discussions with CC management. The ANAO considers that the awareness of privacy issues by call centre staff was high. There appeared to be good liaison and cooperation with APOs and appropriate training was provided to all staff including temporaries.

Recently acquired responsibilities

4.58 In 1998 Centrelink took over the responsibility for paying student and youth benefits. Benefits that were previously paid by the Department of Employment, Education, Training and Youth Affairs under the Austudy program are now paid by Centrelink as the Youth Allowance. The parents of benefit recipients are not automatically allowed to obtain details relating to Youth Allowance payments to their children even though the payments often are made to parents' bank accounts. The ANAO notes that in July 1998 the Privacy and FOI Section provided advice on arrangements under which parents were permitted to inquire in relation to their children's entitlements. Nevertheless, staff at CSCs and CCs indicated during the audit that these arrangements continued to provide difficulties for parents. For example, a parent may ring to enquire why a regular payment made to their bank account (for a child under 18) varied in a particular period. The parent would not be able to obtain advice if the optional section relating to appointment of an agent in the application form had not been completed.

4.59 The ANAO suggests that Centrelink examine the overall arrangements relating to access of parents to information in these circumstances. This should include a review of form design and how staff draw the attention of customers to particular options when they complete the form.

Conclusion

4.60 Given the key role that Area Privacy Officers (APOs) have in the maintenance of privacy and the need for their investigations of privacy breach allegations to stand up to legal scrutiny, the ANAO considers that there is merit in establishing standard induction and related training requirements for new APOs. Concurrently, work standards should be developed for APO operations to promote a consistent and appropriate approach throughout the network.

4.61 Assurance that customer data privacy is being maintained cannot be gained solely through the conduct of investigations of alleged data privacy breaches. Such investigations can only provide a level of assurance in relation to possible breaches actually reported rather than those breaches that may occur but go unreported. To obtain a sufficient level of assurance on this matter, in addition to investigating allegations received, Centrelink should take a more pro-active role in detecting privacy breaches, that is, by actively investigating breaches rather than waiting for allegations to be made. Investigations directed at particular identified risk areas would be a cost/effective means of pro-actively identifying privacy breaches. Oversight of such a pro-active program could be managed by the Privacy and FOI Section in the National Office with key elements of the necessary follow-up being carried out by the business areas.

4.62 The measures used to provide certain customers with additional privacy protection were found to be adequate. However, it was also found that more awareness raising should be provided within Centrelink on the use of customer passwords to improve protection as this simple and effective method could be used more widely than is currently the case.

4.63 The ANAO concluded that processes in place in relation to customer 'aggression tags' were inadequate. These tags are necessary to warn staff of the antipathy that some customers have towards staff. However, they are not always regularly reviewed to ensure that they reflect the most up to date situation and this is inconsistent with the Privacy Principles.

4.64 Paper files, as well as electronic files, contain personal information. The ANAO concluded that possible staff access to paper files and the inappropriate use of the information contained on those files was not routinely considered in the investigation of privacy allegations nor in the provision of update training for staff in Customer Service Centres (CSCs).

5. Management and performance information

This chapter outlines the existing arrangements for performance information and associated issues such as targets, standards and reporting. The arrangements are assessed and one recommendation is made.

Introduction

5.1 Performance information is an essential tool for program management and performance improvement. Suitable, balanced performance information identifies where we are heading, how we will get there, whether we are heading in the right direction and whether we are using resources in the most cost effective manner. As well as providing a basis for informed decision making it is also an early warning system that enables managers to identify problem areas and undertake preventative action. For management purposes, it focuses attention on the factors at the particular manager's level that could influence outcomes. For performance information to achieve these goals, suitable standards and targets must be set, against which performance should be reported.

Performance information

5.2 Performance information for data privacy should relate to specific outcomes and the factors which influence outcomes. In the case of data privacy, while the desired outcomes are not detailed in a specific planning or strategy document they are encapsulated in the terms of reference for the Security and Privacy Committee. Specifically, in relation to data privacy, Centrelink intends to:

- maintain the integrity of security and privacy activities;
- balance business, IT and operational requirements; and
- ensure consistent high quality customer service.

5.3 Performance information should link to these objectives and address important influencing factors such as privacy training.

5.4 Centrelink currently uses the Privacy Allegation Reporting System (PARS) to collect data privacy performance information. The system records the characteristics for each privacy allegation received including:

- type of allegation (for example, browsing or soliciting information);
- use of the computer monitoring system for the investigation;

- number of finalised cases by outcome; and
- referrals for further action (for example, charges laid under the *Crimes Act 1914)*.

5.5 The system also records the details of substantiated allegations, the number of staff attending privacy outreach training sessions and allows comments to be included for each investigation. However, national statistics can only be prepared by manually collating Area statistics. This deficiency has been recognised by Centrelink and the PARS is being redeveloped so that it will have better reporting facilities and provide national statistics in the future.

5.6 Centrelink's current data privacy performance information is detailed in Appendix 3. Information is available at the Area level.

5.7 The ANAO does not consider that Centrelink has a balanced set of performance information. The indicators partially relate to the integrity of data privacy and do not address business issues (such as the efficiency of data privacy operations) or customer service. No information is available on the underlying number of privacy breaches, the time taken to investigate allegations, the quality of the investigations or influencing factors such as privacy outreach training and the effect of these factors on data privacy. These comments parallel matters raised in a previous audit report, *Protection of Confidential Client Data from Unauthorised Disclosure* (Auditor-General Audit Report No. 37, 1997–98), that pointed to a lack of analysis of data and of identification of overall trends in the outcome of investigations.

5.8 The ANAO noted in Chapter 4 (paragraph 4.26) that Centrelink is using pro-active techniques in a limited way to identify privacy breaches. The ANAO considers that similar techniques to those proposed could be used to track the underlying extent of privacy breaches by staff over time. This would constitute a genuine measure of privacy performance. The ANAO was advised that, although pro-active monitoring had previously been considered as a means of collecting information on privacy breaches, it had been discounted as impractical because the volume of material to be analysed would be too large to be interpreted, and the time and resources that it would take to process all of the material reported would require a huge dedication of time and expertise. Centrelink considered that on a risk management basis, such a dedication of resources was not justified.

5.9 The ANAO concurs that this is the case with a traditional monitoring based approach. However, it is considered that the implementation of an appropriate judgemental sample-based approach

could provide performance information. Such an approach could be managed by the Privacy and FOI Section or other business areas with investigations being carried out in the Area offices. This approach would require only marginal additional resources and complement pro-active monitoring referred to in Chapter 4 of this report.

5.10 One way to implement a judgemental sample-based approach would be to select a manageable number of customer records for review each month. This could initially be as low as ten files-datasets with the number selected in future periods being determined in the light of previous experience. Factors that would influence the size of future judgemental samples would be the resources needed for analysis and the number of possible privacy breaches detected. The selection of the files (or datasets) to be reviewed could be random or based on a risk analysis. The work load could be spread over the Areas so that no Area has an inordinately high work load.

5.11 From an operational point of view, IT generated reports that detail who has accessed data, and the sort of access that has been made over the period, would be sent to the Area office. Alternatively, Areas may generate their own reports upon receipt of advice identifying which records should be analysed. Area offices would be requested to verify that:

- all those documented as accessing the data are required to access the data in accordance with their functional responsibilities; and
- the sort of access undertaken such as general enquires, report generation, data modification or deletion, is consistent with the staff functional responsibilities.

5.12 Area offices could then report on the outcome of their investigations to the National Office noting anomalies identified during data checks.

5.13 Besides providing performance information, the implementation of such an approach offers the following possible advantages:

- pro-active monitoring, if properly advertised, represents a deterrent because it introduces a greater possibility that inappropriate activity will be discovered;
- detection of inappropriate data use;
- it would act as a reminder to the business areas and data owners concerning their responsibilities in relation to privacy; and
- there is the possibility that it may highlight data use trends that may be helpful in achieving process efficiencies.

5.14 Centrelink advised the ANAO that the suggested approach is feasible and its implementation would be investigated. Since the initial consideration of the use of pro-active monitoring Centrelink has developed in-house expertise in this type of analysis while undertaking internal fraud investigations. The skills required for fraud investigations and the mechanisms developed would be directly transferable to privacy breach investigations as well as for detecting security breaches. The ANAO notes that the necessary investment in technology is likely to be more attractive if it is able to serve fraud, privacy and security needs.

5.15 Centrelink could also improve performance information by collecting information on customer satisfaction with its efforts to maintain data privacy. This information could be collected in a survey which, to reduce the cost, may be undertaken as part of a more general customer survey.

5.16 Performance information on the quality of allegation investigations and the elapsed time taken to complete the investigation could also be useful. Quality assurance checks are already undertaken on allegation investigations but the outcome of these checks is not reported more broadly than the Privacy and FOI Section in National Office (for example, no report on this is provided to the Privacy and Security Committee). This process could be formalised so that the information collected could be reported as a performance indicator. The information would be useful as it could indicate whether allegations which were 'unsubstantiated' were reported in this way because they were unfounded, there was insufficient evidence, or the investigations were inadequate.

5.17 Currently, no statistics are produced on the elapsed time for investigations. These data would be a useful indicator as, from both Centrelink's and a customer's perspective, it is highly desirable that complaints be dealt with quickly. Consistently short and long investigation times within an Area should be explained as they could indicate that an APO has inadequate time to deal with investigations and/or may not be giving complaints sufficient attention. Centrelink has recognised the importance of investigation time and the Privacy Breach Allegation Investigations Procedures Manual specifies that the investigations should be completed within 60 days of the initial report. However, it is understood that information on whether this target has been met is not reported or analysed because of deficiencies in PARS. Centrelink has advised the ANAO that a revised version of PARS will allow the collection of such data.

Targets and standards

5.18 Performance information provides the foundation for performance monitoring and assessment. However, performance information in its own right is insufficient for performance assessment as standards, targets, benchmarks and milestones are necessary to provide the basis for comparisons.

5.19 The only performance information standard or target relevant to data privacy identified by the ANAO is the requirement that investigations be completed within 60 days of a breach being reported. As mentioned above (paragraph 5.17), while this standard exists, no information is collected on performance against this standard.

5.20 The ANAO considers that, in order to assess Centrelink's performance, standards and targets are necessary for all indicators. These standards and targets should be used to compare the performance over time and between various Areas and, in the longer term, consistent with Centrelink's organisational objective, benchmark the agency's performance against that of comparable organisations.

Recommendation No.11

5.21 The ANAO recommends that Centrelink:

(a) review the performance information for data privacy and develop indicators that provide an effective means of monitoring and assessing data privacy outputs and outcomes and the principal factors that influence the achievement of the desired results; and

(b) set performance standards and targets against each indicator and, where possible, identify suitable comparative benchmarks.

Centrelink's response:

5.22 Agreed. Centrelink is implementing an enhanced Privacy Incident Reporting System which will be used to determine success in achieving privacy outcomes. The system has capacity to record and measure the actual number of privacy breaches and will be useful in determining and defining criteria for monitoring and in reporting to internal and external organisations.

Reporting

5.23 Performance information reports provide the basis for internal management monitoring and decision making and the means by which external accountability is achieved. To meet the needs of a variety of audiences a number of reports must be produced with different levels of detail and a different balance of measures.

5.24 Within Centrelink, relevant to data privacy, internal management reports are generated using PARS information. Audiences external to Centrelink primarily obtain their information through the Annual Report.

5.25 Currently, it is time consuming to use PARS information to generate reports as it does not have statistical or report generation facilities. However, Centrelink is aware of these deficiencies and PARS is being further developed. The project plan for the redevelopment of PARS includes improved reporting facilities. The ANAO supports the development and implementation of such systems which allow the easy preparation of routine and ad hoc reports.

5.26 PARS information is used by some offices for local management reports detailing progress on outstanding allegation investigations. These reports are used to monitor the number and status of allegation investigations. The ANAO considers that there would be merit in all Areas determining their local data requirements and producing appropriate reports.

5.27 The *Privacy Allegation Statistics* report is the primary source of information on data privacy within Centrelink. It is created, in the most part, from information in PARS which currently must be manually collated. The report is considered by Centrelink's Security and Privacy Committee at each quarterly meeting. It has information on:

- investigations finalised;
- type of all allegations received;
- source of all allegations received;
- criminal charges;
- use of the information technology access logging system (CRAM) for breach investigations;
- mailhouse problems such as misdirected mail; and
- privacy training and outreach activities.

5.28 While the report is useful, there is considerable scope for it to be improved. Following are some suggestions which could improve the reports produced:

- the presentation of data in graphical / pictorial form;
- the inclusion of additional information on data privacy such as the efficiency of data privacy operations, the underlying number of privacy breaches and factors influencing the quality of investigations of privacy allegations;
- the comparison of Areas according to critical parameters; and

- the inclusion of a qualitative overview of the status of data privacy in Centrelink.

5.29 Improvements in performance indicators as discussed earlier are essential to ensure that the effectiveness of data privacy can be properly determined and monitored. As the Areas have quite different customer populations and geography, care must be taken when comparing Areas. It is, therefore, essential that reports have qualitative discussions which identify and explain problems. In addition, qualitative discussions should explain statistics and trends and address information validity and reliability.

5.30 Centrelink's external accountability in relation to data privacy is primarily achieved through the Annual Report. The Report has statistics on:

- substantiated, unsubstantiated and unsubstantiated/withdrawn allegations;
- allegations by breach offence type; and
- referrals for further action (Australian Federal Police, personnel disciplinary action, Director of Public prosecutions and industrial relations).

5.31 The Annual Report also has background material on privacy allegations, the automatic logging of access to customer records and referrals for further action.

5.32 The ANAO considers that there is scope to improve the usefulness of information contained in the Annual Report in the following ways:

- the inclusion of information for a more 'balanced' set of indicators covering the efficiency and quality the investigations of privacy allegations, as well as the underlying number of privacy breaches;
- the determination and reporting of data privacy trends;
- a discussion of Centrelink's (privacy) performance relative to standards, targets and benchmarks if suitable benchmarks can be found.

Conclusion

5.33 The ANAO concluded that Centrelink does not have a satisfactory range of performance indicators for data privacy and, therefore, is unable to properly determine its success in achieving privacy outcomes. For example, performance information does not include indicators that enable the measurement of the actual number of privacy breaches by staff. The range of indicators for which information is collected should be appropriately expanded and consideration should be given to pro-actively

collecting, monitoring and reviewing information on the underlying rate of privacy breaches. Appropriate targets and standards should be set for all indicators for management and accountability purposes.

5.34 The ANAO also concluded that the internal and external reporting on data privacy was inadequate. While the narrow range of indicators for which information is collected contributes to the inadequacy of the reports, consideration should also be given to the various means by which the reports themselves could be made more useful. For example, management reports should include qualitative analyses, the presentation of data in a form that makes it more readily understandable to users and the provision of information on the trend in data privacy breaches over time.

Canberra ACT
23 August 1999

P. J. Barrett
Auditor-General

Appendices

Appendix 1

Abbreviations/Glossary

ACF2	A software facility that controls user access to mainframe systems
ACM	Accelerated Claimant Matching—internal consistency checks of customer information against other information held by Centrelink
ADMINS	Centrelink's HR system—ADMINS, tracks staff members and their occupancy against agency positions. ADMINS is due to be replaced by SAP HR by July 1999
AFP	Australian Federal Police
APO	Area Privacy Officer
AS 4390	The Australian Standard for records management
ATO	Australian Taxation Office
CC	Call Centre—a Centrelink office dedicated to handling telephone inquiries
Code walkthrough	Following the completion or drafting of a section of computer code, a walkthrough is the process of following an example of every item and variable addressed or created by the code from its origin to its final destination. This process may be undertaken manually or with the assistance of automated testing tools specifically designed to 'step through' code instruction by instruction
Computer code	Computer code is an individual instruction or sequence of instructions designed to produce a specific effect within a computerised processing environment. The specific effect may be the storage, retrieval, addition, deletion or movement of data or the change of a logical or physical state. For example, activating or deactivating a computerised device
CRAMS	Customer Record Access Monitoring System—a computer system that records each access to sensitive Centrelink information. It has details on the customer whose records were accessed, the Centrelink staff member involved, screens accessed and when the access occurred. Reports can be generated for specific staff members or customers

CSC	Customer Service Centre—a Centrelink office that is the primary customer contact and service delivery point
Data Matching Program	The comparison of Centrelink customer information with that held by the Department of Employment, Workplace Relations and Small Business, ATO and Department of Veterans' Affairs. Tax file numbers are used to match records and the legislative basis is the *Data-matching Program (Assistance and Tax) Act 1990*
Deny Access Facility	A mechanism that provides additional protection for information on 'sensitive' customers. For example, customers in a witness protection scheme or at risk of domestic violence
DMIS	Debt Management Information System—a computer-based system that records details of debts arising from overpayments
EDF	Employment Declaration Form
EII	Enhanced Investigation Initiative—the visual (sometimes referred to as optical) surveillance of customers by private investigators
EP63	A registration system for violent or abusive customers
ESAS	Education Studies Assistance System—a computer system used to support Austudy payments
FOI	Freedom of Information
IES	Integrated Employment System—a Department of Employment, Education, Training and Youth Affairs / Department of Employment Workplace Relations and Small Business system that has jobseeker information
IPP	Information Privacy Principle—detailed in the *Privacy Act 1988*
ISIS	Income Security Integrated System—also known as Common Platform—identifies common activities across Income Support Systems (Pensions, Parenting, Newstart and Families) and writes programs for each activity (for example, customer registration) which can be used by all systems
IT	Information Technology
JNRT	Job Network Referral Targets

Model 204 database	This is the strategic database that all income support systems have used since the implementation of the Newstart Common Platform in April 1998
MOU	Memorandum of Understanding
National Index	A means by which all new customer records are automatically checked to determine if they already exist in any Centrelink system
National Selective Review	Records the results of compliance reviews performed by Centrelink for income support payments
PAC	Procedure and Accuracy Check—the quality and assurance package used by Centrelink to promote data accuracy. It requires a 100 per cent check for new staff and a 10 per cent random check for other staff
PARS	Privacy Allegation Reporting System—a computer-based system used by Privacy officers to record information on privacy allegation investigations
PAS	Privacy Allegation System—the predecessor to PARS
PI	Privacy Incident
PIR	Privacy Incident Record
POI	Proof of Identity
PPS	Prescribed Payments System—a prescribed payment is a term used by the ATO to mean a payment made under a contract which, wholly or partially, is for work in specific industries. Some of the industries involved are: building and construction, cleaning, engineering services, motor vehicle repair and road transport. The Prescribed Payments System is a means by which these people can pay their tax in steps throughout the year
Privacy Awareness Kit	A set of papers prepared by the Privacy and FOI Section of Centrelink to help staff understand their responsibilities and the Agency's in relation to privacy and confidentiality. It includes the *Confidentiality Manual*, *Breaches of Privacy and Confidentiality Manual*, *Privacy Manual* and current *National Instructions* on privacy and confidentiality matters

RPS	Reportable Payments System—a reportable payment is a term used by the ATO to mean a payment made under a contract for the supply of goods in specific industries. Industries covered are fruit and vegetable, clothing, fishing and smash repair. The Reportable Payments System is an income reporting system whereby certain payments made to people in these industries are to be reported to the Australian Tax Office. It also covers people who fail to provide their tax file number.
SAMS	Security Access Management System—a computer system that is used to manage ACF2 access
TFN	Tax File Number
TORS	Tip off Recording System—a computer-based system used to manage information received on customers who, complainants allege, may not be entitled to the benefits that they receive

Appendix 2
Information Privacy Principles

IPP 1: *Manner and purpose of collection of personal information*

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:

a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and

b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information shall not be collected by a collector by unlawful or unfair means.

IPP 2: *Solicitation of personal information from individual concerned*

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

(c) the purpose for which the information is being collected;

(d) if the collection of the information is authorised or required by or under law—the fact that the collection of the information is so authorised or required; and

(e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

IPP 3: *Solicitation of personal information generally*

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances,

reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

IPP 4: *Storage and security of personal information*

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

IPP 5: *Information relating to records kept by record-keeper*

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) whether the record-keeper has possession or control of any records that contain personal information; and

(b) if the record-keeper has possession or control of a record that contains such information

  (i) the nature of that information;

  (ii) the main purposes for which that information is used; and

  (iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:

(a) the nature of the records of personal information kept by or on behalf of the record-keeper;

(b) the purpose for which each type of record is kept;

(c) the classes of individuals about whom records are kept;

(d) the period for which each type of record is kept;

(e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and

(f) the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:

(a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

(b) give the Commissioner, in the month of June in each year, a copy of the record so maintained

IPP 6: *Access to records containing personal information*

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

IPP 7: *Alteration of records containing personal information*

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

(a) is accurate; and

(b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

3. Where:

(a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

(b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth.

the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

IPP 8: *Record-keeper to check accuracy etc. of personal information before use*

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

IPP 9: *Personal information to be used only for relevant purposes*

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

IPP 10: *Limits on use of personal information*

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

(a) the individual concerned has consented to use of the information for that other purpose;

(b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

(c) use of the information for that other purpose is required or authorised by or under law;

(d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

(e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

IPP 11: *Limits on disclosure of personal information*

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

(a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

(b) the individual concerned has consented to the disclosure;

(c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;

(d) the disclosure is required or authorised by or under law; or

(e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

Appendix 3

Centrelink data privacy performance information

Measure	*Performance 1997–98 (unless otherwise stated)*	*Type*	*Description*
1. Privacy breaches Privacy allegation investigations	970	input (process)	the number of allegations received in a given period (total and by type of breach)
Privacy outreach training sessions—staff attending	801 staff attended training (January to March 1998)	Centrelink people key result area	the number of staff attending privacy outreach training sessions conducted by privacy officers
Allegation investigations using ADP monitoring	733	process	the number of allegations investigated using CRAMS
Outcome of investigations and and outstanding cases • finalised • withdrawn	970 completed 210 substantiated (table below) 760 unsubstantiated/ withdrawn	process	the number of finalised and outstanding allegation investigations with cases referred for further action identified by type of action
2. Mailhouse Mailhouse problems	13 incidents (January to March 1998)	process	the number of dual and misdirected mailhouse incidents reported to Centrelink

Referrals for action for substantiated allegations

Referral for action	*Performance 1997–98*
Australian Federal Police	8
Personnel disciplinary action	116
Director of Public Prosecutions	30
Industrial Relations	1
Awaiting decision on how to proceed	55
total	210

Index

A

ACF2 17, 45, 47, 48, 73, 76
ADMINS 47, 73
aggression tags 14, 62
Area Privacy Officers (APOs) 13, 34, 51-54, 58-61, 66, 73

C

Crimes Act 9, 24, 26, 64
Customer Record Access Monitoring System (CRAMS) 31, 48, 54, 55, 73, 82

D

Deny Access 56

F

Freedom of Information Act 9, 24

I

Income Security Integrated System (ISIS) 54, 58, 74
Information Privacy Principles (IPP) 9, 10, 23-26, 40, 43, 45, 77-81

M

Model 204 44, 48, 75

P

performance information 10, 14, 19, 28, 48, 53-55, 63-67, 69, 82
Privacy Allegation Reporting System (PARS) 63, 64, 66, 68, 75
Privacy Act 9, 10, 12, 24-26, 28, 29, 36, 39, 40, 49, 56, 65, 78
Privacy and FOI Section 12, 14, 16, 29-35, 37, 51-55, 61, 62, 65, 66, 75
Privacy Commissioner 9, 23, 25-30, 36, 41, 60

S

SAS 42, 74
Security Access Management System (SAMS) 42, 47, 48, 76
Security and Privacy Committee (SPC) 30, 32
Social Security Act 9, 25-27, 29

Series Titles

Titles published during the financial year 1999–2000

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

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

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

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

Audit Report No.5 Performance Audit
IP Australia—Productivity and Client Service

Audit Report No.6 Audit Activity Report
Audit Activity Report January to June 1999
Summary of Outcomes

Audit Report No.7 Protective Security Audit
Operation of the Classification System for Protecting Sensitive Information

Better Practice Guides

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