Commonwealth Department of Family and Community Services

Submission to the Joint Committee of Public Accounts and Audit (JCPAA)

Inquiry into the *Management and Integrity of Electronic Information in the Commonwealth*

INTRODUCTION

The Family and Community Services portfolio consists of the Department of Family and Community Services (FaCS), Centrelink and the Australian Institute of Family Studies (AIFS). FaCS incorporates the Child Support Agency (CSA). The resources needed to support the operations of the Social Security Appeals Tribunal are also provided through FaCS. A brief agency description follows:

- the CSA - a semi-autonomous agency within the portfolio that promotes parental responsibility for the costs of raising their children and provides services to help parents pay child support.
- Centrelink - a service delivery organization, responsible for providing Commonwealth Government information, products and services to the Australian community.
- AIFS - an independent statutory authority that promotes the identification and understanding of factors affecting marital and family stability in Australia.

2. FaCS is the principal policy formulation and advising body in the portfolio. The Department was formed in October 1998 with a vision of building a modern social safety net to bring about a fair and cohesive Australian society. FaCS has a broad range of responsibilities including responsibility for implementing the Government's income security policies and delivery of services for people with disabilities, families with children, community support, family relationships and welfare housing.

3. Our programmes and services are delivered by third party organizations. Centrelink, as our principal service delivery provider, delivers all income security policies and payments to customers on our behalf. Services for people with disabilities, families, community support, family relationships and welfare housing are delivered by a combination of government agencies and non-government organizations (NGOs) - including private sector and community organizations.

4. This submission incorporates the views and operations of the Department and the CSA. Centrelink has lodged its own submission to the Inquiry.

A. PRIVACY, CONFIDENTIALITY AND INTEGRITY OF THE COMMONWEALTH'S ELECTRONIC DATA

5. FaCS' portfolio legislation contains strict confidentiality and secrecy provisions regulating authorised uses of customer information, which applies regardless of the medium in which the data

is held. The current provisions are considered adequate. Strict penalties apply and are enforced if there are breaches of customer confidentiality. Our agencies have in place mechanisms to manage electronic data held on systems including client, financial management and human resource databases to ensure privacy and security of the data is managed in accordance with portfolio and statutory obligations.

6. All changes to FaCS' systems must go through the FaCS Change Committee. This Committee requires that privacy considerations are examined and accepted by the Agency Privacy Officer.

7. Customer data associated with FaCS' income support programs and services delivered by Centrelink is collected and maintained by Centrelink and held in their computer systems. In the main, customer data is held in the mainframe. FaCS is recognised as the joint record keeper with Centrelink for this data and uses it to carry out accountability, reporting, policy research and development, program monitoring and public disclosure responsibilities.

8. The working relationship between FaCS and Centrelink is set out in the FaCS/Centrelink Business Partnership Agreement 2001-2004 (the BPA).

9. The Business Development and Operations Protocol of the BPA governs access to data. Section 14 sets out the management framework for Centrelink to provide information and data services to FaCS and the management information outputs required by FaCS. In particular, Section 4 sets out the roles and responsibilities for the provision of management information and the need to work cooperatively to ensure it is delivered in a cost effective manner. In order to formalise the administrative arrangements for access to data, a Memorandum of Understanding (MoU) is being developed to cover the access of authorised FaCS staff to Centrelink electronic files and data sets.

10. FaCS program branches monitor the integrity of data. If significant errors or omissions are found, a "Request to Correct" is the agreed method for alerting Centrelink. A Key Performance Indicator (KPI) has just been agreed between FaCS and Centrelink to monitor Centrelink's performance – 'the provision of accurate data'. We are currently working with Centrelink to put in place a suitable mechanism for verifying the information provided as part of this KPI.

11. FaCS, in conducting its day-to-day business, has three business drivers relating to this Inquiry's terms of reference, they are:

- ***Ensuring the privacy, confidentiality and integrity of information provided to stakeholders by FaCS***

  In recent years, a number of important departmental initiatives have been aimed at expanding the quantity and quality of unit record data[1] available to analyse the impacts of FaCS departmental initiatives and policies. FaCS has in place policies to manage security of unit record data and to ensure that privacy of individuals is not breached.

  Access to, and use of, unit record data by FaCS staff and researchers who FaCS has either commissioned or approved to undertake research is managed through documented policies endorsed by the FaCS Research and Evaluation Committee. These policies set out procedures and minimum conditions under which staff or researchers may access and use FaCS unit record data.

  The Commonwealth Protective Security Manual (PSM) and Australian Communications-Electronic Security Instruction 33 (ACSI33), which cover procedures and controls to be put in place to protect Commonwealth material, provide the basis for FaCS policies in regard to access to, and use of, unit record data.

  In accordance with the PSM, before unit record data is released, it is given an appropriate security classification. The security classification guides the level of security that is required. The FaCS Longitudinal Administrative Data Set, for example, has been classified as X-in-confidence because it has not been confidentialised and has the potential for individual customers to be identified.

  All unit record data has a business owner in FaCS who is responsible for implementing and monitoring access to it.

[1] Unit record data refers to files that contain records of individual customers or households. Each line or series of lines of unit record data represents data on an individual or household.

FaCS security protocols and procedures also apply to access to unit record data by FaCS staff. Some datasets are stored in shared folders and individuals must apply to get access to them through the business owner or their delegate. Small unit record datasets from surveys or other research are stored in individual branch folders and are password protected.

FaCS provides external access to its unit record data using a number of channels. These include the Social Policy Research Contracts/Australian Research Council Linkage Grants; commissioned research and non-commissioned research. All of these are covered by licenses or contracts whose specific details vary. However, all these agreements include clauses covering intellectual property rights, rules for publishing, data security requirements and confidentiality and standard mechanisms that can be used for dealing with complaints relating to the breach of individuals' privacy. Access to unit record data is only given to approved individuals who have executed a Deed of Confidentiality and a Deed of Non-disclosure.

FaCS has received a number of requests from other Commonwealth departments such as the Department of Employment and Workplace Relations (DEWR) for access to its unit record data. In these cases FaCS does not stipulate any particular security requirement beyond drawing the agency's attention to their obligations under the PSM and ACSI33 in a MoU or other agreement that covers the release of the dataset. FaCS uses the following procedure to transfer the Jobseeker Dataset from FaCS to DEWR.

When X-in-confidence data is provided to an external agency or department, formal procedures that ensure the security of the data while in transit, are followed. These procedures include encrypting the data, putting a secure password on the file and delivering the data either by hand or secure courier.

FaCS' policies for access to its unit record data have been developed for both internal and external users.

- ***Ensuring the privacy, confidentiality and integrity of information collected by other organizations on FaCS' behalf***

  As a Government agency, Centrelink is bound by the same stringent privacy and confidentiality conditions as FaCS in collecting, using and storing electronic data for the purposes of administering income support payments on FaCS' behalf.

  FaCS requires other service providers to comply with privacy and confidentiality requirements and uses clauses in legal documents as a condition of receiving funding from FaCS to deliver programmes and services on our behalf. The Department has established several mechanisms for checking provider compliance in this area.

- ***Ensuring the privacy, confidentiality and integrity of FaCS' information storage (both in the short and long-term)***

  A FaCS-wide Business Continuity Framework has recently been developed to ensure that FaCS can manage and recover from emergencies, disasters and other disruptive events.

  The Framework includes the establishment of a command structure (with supporting recovery teams) as well as high level strategies and detailed plans/procedures for key risk areas of FaCS (including payment systems, accommodation, IT and cyclone prone offices). In the case of IT, the Business Information Solutions Branch as part of a longer term Business Continuity Management project has developed a disaster recovery plan.

  This project has identified, through disaster scenario testing, the existing capabilities, requirements and weaknesses within the existing environment. A number of recommendations for improvement were made addressing single points of failure, quality and management of disaster recovery documentation and other risks to the recovery process. Future phases of the project will address these recommendations

  It is proposed that FaCS' Business Continuity Framework will be tested by a simulation exercise in 2003.

FaCS' holds the view that the Commonwealth in general needs to pay greater attention to the preservation and access of data holdings over time. There is no whole of government strategy or resources for identifying data sources across agencies that need to be preserved over long periods of time. There is also a need to ensure that such data remains accessible over changes of technology including software.

CSA response

12. Only staff and/or contractors who have a business need to access electronic data are provided with such a facility.

13. Staff and contractors who are required to have access to confidential electronic data, are permitted access to CSA premises or information via a formal security clearance, an initial pre-engagement character check and a signed declaration of secrecy. The continuing requirement and suitability of staff with security clearances at the protected level or higher is reviewed annually.

14. Access to CSA premises is via a building pass. Staff are required to wear their building pass in a visible manner at all times while on CSA premises.

15. CSA has a strong privacy culture. New staff are provided with privacy and secrecy training as part of their induction to the CSA and are made aware of the confidentiality provisions in the *Child Support Act* and the *Privacy Act*. Security and privacy information is also made available to staff via the CSA intranet site.

B. MANAGEMENT AND SECURITY OF ELECTRONIC INFORMATION TRANSMITTED BY COMMONWEALTH AGENCIES

16. FaCS maintains a website (www.facs.gov.au) primarily for information dissemination to members of the public. We also operate a small number of on-line transactional systems that enable a limited ability for stakeholders to interact electronically. We are currently evaluating the implementation of further electronic services to help improve our service to customers (an example being the ability for external stakeholders to order departmental publications on-line). Programme managers within FaCS are responsible for maintaining the accuracy of their programme's information on the website.

17. A major initiative from the Government Online Strategy is the whole-of-government portals framework. FaCS is one of the major contributors to the Portals Framework, being the lead agency for three portals – Families, Communities and Youth – which are each administered by specialist areas within the Department. There are a number of other portals administered by the Department that support the three portals listed above. FaCS is also a member agency on the regional, employment, Indigenous, senior's and women's portals. The portals framework aims to provide government information and services in a seamless, integrated and customer-focussed manner, based on subject and customer groupings.

18. FaCS takes the threat of external interference to its infrastructure very seriously. FaCS Web Servers are hosted by service provider 90East, the Government endorsed and Defence Signals Directorate (DSD) certified Internet gateway environment. This environment provides physical security for hardware storage, processing and transmitting Commonwealth information classified up to and including Highly Protected. This physical environment as well as the logical security provided by numerous DSD approved firewalls and encryption affords adequate protection for FaCS/Commonwealth information from external interference.

19. The likelihood for internal error as it relates to information management is greatly reduced by the fact that establishment of most web sites within the Department is managed centrally.

20. During 2002, FaCS reviewed 14 of its web sites using the checklist contained in the National Office for the Information Economy (NOIE) Internet Delivery Decisions Guide. Business Owners were provided with a report on their web site and copies of all reports were provided to the Audit & Assurance Branch for their information. Recommendations arising from the reports have been summarised and are being actioned for inclusion in the FaCS Security Action Plan.

21. FaCS has acknowledged all recommendations contained in the Australian National Audit Office (ANAO) Audit Report No. 13, 2001-02, *Internet Security within Commonwealth Government*.

CSA response

22. The majority of electronic information transmitted by the CSA is to internal CSA/Australian Taxation Office (ATO) sites. This is done through the ATO internal network, which is heavily protected and closely managed. Data relating to mutual customers is transmitted to Centrelink through the CSA/Centrelink interface after encryption.

23. At present the CSA does not conduct e-business.

C. MANAGEMENT AND SECURITY OF THE COMMONWEALTH'S ELECTRONIC INFORMATION STORED ON CENTRALISED COMPUTER ARCHITECTURE AND IN DISTRIBUTED NETWORKS

24. FaCS is revising its IT Strategic Plan and the Technical Architecture (a sub-component of the plan) to reflect the Department's desire to increase its alignment with the Government's whole-of-government approach and to take advantage of significant reengineering of some of FaCS' key systems. A strong theme in both documents is governance of IT processes and greater visibility of the impact of change on the IT environment. This governance theme includes monitoring of infrastructure services provided through a multi-vendor environment.

25. FaCS is implementing a range of projects to further ensure the security of information held on the departmental network, these include:

- encryption of the FaCS Wide Area Network;
- improvements in event logging and intrusion detection; and
- more secure remote access facilities.

26. There is significant cost associated with the classification of data as per the PSM. This is a key consideration for the management and security of information stored in distributed networks. In FaCS' case, the greatest exposure is data stored on distributed networks by NGO service providers. Ensuring that data is classified correctly and stored appropriately in line with stringent Government requirements is a key priority for FaCS (and other agencies). To ensure that service providers are equipped to do so and are given the necessary resources to comply is a whole of government priority that calls for a consistent approach – given that the delivery of most Government services is contracted to other organizations.

CSA response

27. Electronic information of a sensitive nature is stored in two places, either the mainframe or on internal servers. Access to customer information, which is stored on the mainframe, is permitted through RACF security. Information stored on servers can be accessed through network security. Two System Administrators manage these systems.

28. Electronic audit trails are carried out for mainframe activity. The Fraud Prevention and Control team monitors this information.

D. ADEQUACY OF THE CURRENT LEGISLATIVE AND GUIDANCE FRAMEWORK

29. FaCS, as a Commonwealth Government agency, complies with the Information Privacy Principles contained in the Privacy Act. For example, the FaCS web site and portals clearly sets out our policy in relation to the online handling of personal information. We also provide a Copyright notice and disclaimer to the information contained on our web site. The Department abides by all other legislation governing the delivery of electronic services. The existing legislative framework is adequate for the environment in which FaCS operates at present.

30. FaCS is keen to take a lead role in the developing e-Government guidance framework. We are keen participants in whole of government activities sponsored by NOIE and have committed ourselves to be active participants in the recently established Information Management Strategy and the Chief Information Officer Committees as part of the Management Advice Committee *Australian Government Use of Information and Communications Technology – A New Governance and Investment Framework Strategy*. This strategy provides a framework for guiding Commonwealth departments and agencies through the transformation of current business processes to adopt and respond to new technologies.

31. We want FaCS to be a lead agency in the use of innovative business solutions to support organisational outcomes. We are developing strategies to utilise evolving IT opportunities to support more flexible ways of working into the future (this includes a greater understanding and use of assistive technology). We intend to present a discussion paper for the consideration of NOIE and other stakeholders in the first quarter of 2003 explaining the strategy we intend to pursue. We will also discuss existing barriers that inhibit us and other organizations from using innovative IT solutions.

32. Our primary function is to develop policy that provides flexible and responsive solutions to underpin the Government's social policy and welfare reform agenda. We cannot achieve our vision of building stronger families and communities on our own – we must work in partnership with communities and business in the development and implementation of good policy. Our work on Australians Working Together and the Family Assistance Office are practical examples of our achievements.

33. Likewise, we understand the value of having effective service delivery systems in place to deliver good policy to those who require it most. Our big challenge is to support others in providing sophisticated service delivery solutions to customers (given that we do not conduct direct service delivery provision ourselves). The cost to service providers in meeting stringent compliance requirements for the electronic collection, usage and storage of information collected on our behalf will continue to be a critical issue requiring careful management.

CSA response

34. The existing legislation relating to protection and management of electronic information and client identity management requires a great deal of judgement to apply to our system. Additional clarity and guidance about issues such as electronic signatures, physical protection of networks, intruder detection and so forth would be valuable.

CONCLUSION

35. The three key issues arising from this submission are:

- the cost of compliance to NGOs for managing electronic information in compliance with stringent Government regulations;
- the "tensions" arising from managing stringent security requirements and the deployment of more flexible approaches to work and service delivery; and
- the need for a whole of government approach to the long-term preservation of, and access to, electronic information.

36. FaCS and the CSA would like to thank the Committee for giving us the opportunity to lodge this submission to the Inquiry into the Management and Integrity of Electronic Information in the Commonwealth.