Reference No: JPCAA_EP63/2003/06942
Business and Information Protection
PO Box 7788
Canberra Mail Centre ACT 2610

Telephone: (02) 6219 8340
Fax: (02) 6219 8481

Secretary
Dr John Carter
Joint Committee of Public Accounts and Audit
Parliament House
Canberra ACT 2600

18 June 2003

Dear Dr Carter,

Management and Integrity of Electronic Information in the Commonwealth

On Monday 31 March, Centrelink attended an inquiry into the *'Management and Integrity of Electronic Information in the Commonwealth'*. The Committee sought the following information:

1) A complete list of the organisations that Centrelink matches data with; *(Transcript, page 21)*
2) A complete list of organisations that Centrelink exchanges information with under social security legislation; *(Transcript, page 21)*
3) Details of Centrelink's processes for applying and reviewing aggression tags; *(Transcript, page 25)* and
4) A significant amount of Centrelink data is held on hardware owned by private companies and leased to Centrelink. How does this ownership arrangement affect your security policies, especially concerning the issues of redundancy and disaster recovery? *(Transcript, page 29)*
5) What action is Centrelink taking to guard against social engineering?
6) What action is Centrelink taking to ensure the long-term archival integrity of its data?

1. Organisations Centrelink matches data with:

The Data-Matching Agency checks that the information people give about their identity and income is consistent with the information they give other participating agencies. This matching is authorised by *the Data-matching Program (Assistance and Tax) Act 1990*. The participating agencies are Centrelink**,** the Department of Veteran's Affairs and the Australian Taxation Office.

The following agencies are involved in Centrelink's non-legislative or "other" data-matching projects:

- Australian Taxation Office (ATO);
- Department of Immigration, Multicultural and Indigenous Affairs (DIMIA);

- State and Territory Departments of Corrective Services;
- Educational institutions in all states and territories, as well as private providers of education and training;
- Defence Housing Authority;
- Commonwealth Superannuation Authority;
- Registrars-General of Births, Deaths and Marriages in all states and territories;
- Australian Securities and Investment Commission (ASIC)**;** and
- Department of Employment and Workplace Relations (DEWR)**.**

Department	**What is matched**
ATO	To detect incorrect income support payments
DIMIA	To detect customers who have left Australia without notifying Centrelink of their intended absence prior to departure
Corrective Services	Detect cases where customers have been incarcerated
Educational Institutions	Detects customers who are receiving assistance to study to ensure they are enrolled and meeting workload and attendance requirements.
Defence Housing Authority	Detects customers who are incorrectly receiving Centrelink payments while living at DHA residences.
Commonwealth Super Authority	Detects customers who have received income from the Commonwealth Super Fund and have not disclosed this income, or have incorrectly disclosed this income.
Births, Deaths and Marriages	Addresses the risk of ongoing payment where the death of a customer, their partner or their child is not reported to Centrelink
ASIC	Detects customers who have failed to declare share holdings in small proprietary companies and non-listed public companies.
DEWR	Detects customers who have commenced employment other than full time and have failed to declare or incorrectly declare income from employment.

2. Organisations that Centrelink exchanges information with under social security legislation:

The Chief Executive Officer of Centrelink has issued Certificates of disclosure under section 208(1)(b) of the *Social Security (Administration) Act 1999* and section 168(1)(b) of the *Family Assistance (Administration) Act 1999* for each of the following departments:

- Comcover - a branch within the Department of Finance and Administration;
- Aboriginal and Torres Strait Islander Commission;
- Administrative Appeals Tribunal;
- Attorney-General's Department;
- Australian Electoral Commission;
- Australian Federal Police;
- Australian Government Solicitor;
- Australian Taxation Office;
- Child Support Agency;
- Comcare Australia;
- Commonwealth Director of Public Prosecutions;
- Commonwealth Ombudsman;
- Department of Defence;
- Department of Education, Science and Training;
- Department of Employment and Workplace Relations;

- Department of Health and Ageing;
- Department of Immigration, Multicultural and Indigenous Affairs;
- Department of Veterans'Affairs;
- Health Insurance Commission;
- Social Security Appeals Tribunal; and
- Torres Strait Regional Authority**.**

Department	**Purpose 'in brief'**
Comcover - a branch within the Department of Finance and Administration	To assist in determining whether Centrelink is legally liable to compensate a person for economic loss which is claimed to have resulted from negligence on the part of Centrelink.
Aboriginal and Torres Strait Islander Commission	For the purpose of the Community Development Employment Program.
Administrative Appeals Tribunal	For processing applications for review under the *AAT Act 1975.*
Attorney-General's Department	For the purpose of requesting legal advice and carrying out obligations under the Hague Convention.
Australian Electoral Commission	For the purpose of maintaining the integrity of the electoral roll.
Australian Federal Police	To investigate offenses under social security and family assistance law.
Australian Government Solicitor	For the purpose of requesting legal advice.
Australian Taxation Office	For income and tax related matters.
Child Support Agency	For the purpose of the administration of the *Child Support Act.*
Comcare Australia	For investigations under the *Occupational Health and Safety (Commonwealth Employment) Act 1991.*
Commonwealth Director of Public Prosecutions	To assist with the prosecutions or possible prosecutions for offenses under social security law, family assistance law and/or the *Criminal Code Act 1995.*
Commonwealth Ombudsman	For the purpose investigation of complaints or 'own motion' enquiries.
Department of Defence	To assist in the administration of the provision of housing assistance to members of the Australian Defence Force and their dependents.
Department of Education, Science and Training	For the administration of various programs.
Department of Employment and Workplace Relations	For the administration of various programs in relation to jobseekers.
Department of Health and Ageing	To validate data received from an eligible person for participation in the voucher system specified in the *Hearing Services Administration Act 1997* and for the calculation of residential care fees..
Department of Immigration, Multicultural and Indigenous Affairs	For the purpose of Assurances of Support and unlawful entry into Australia.
Department of Veterans' Affairs	To calculate or determine a payment where a person or their partner is transferring to or from a social security payment.
Health Insurance Commission	To verify eligibility under the Pharmaceutical Benefits Scheme.
Social Security Appeals Tribunal	For the purpose of carrying out the functions of the Tribunal under the Act.

Torres Strait Regional Authority	For the purpose of the Community Development Employment Program.

3. Customer Aggression Tags:

The 'tag' or indicator is not used indiscriminately or for every customer who is or has been the subject of a customer aggression report. Rather, it indicates those customers who frequently exhibit some form of aggressive behaviour or who have been involved in an act of violence involving Centrelink, for example assault, or property damage.

The indicator is held on the customer record and serves as an alert for an employee to the customer's previous aggressive behaviour. Office Managers determine whether a customer's behaviour warrants the input of an indicator. This decision is made in consultation with relevant employees and takes into account:

- the nature of the customer's behaviour,
- the customer's previous behaviour in the office or other offices, and
- any extenuating circumstances that contributed to the incident and are unlikely to be repeated.

Under common law, Centrelink has a duty of care to provide a safe working environment for its employees. It also has obligations under the *Occupational Health and Safety (Commonwealth Employment) Act 1991* to take all reasonably practicable steps to protect its employees' health and safety while they are at work.

As a result of these responsibilities to employees, **the deletion of customer aggression indicators is a matter for the Customer Service Centre manager to decide**, keeping in mind the following factors:

- the length of time since the customer's last aggressive incident,
- the customer's behaviour since the previous incident,
- the nature of the customer's aggressive behaviour, and
- the opinions of those officers who are dealing with the customer at present.

The existence of a customer aggression indicator on the customer's record does not influence an employee's decision in respect of that customer. Centrelink's Customer Aggression Guidelines are now under review as part of Centrelink People Management Handbook rewrite.

4. A significant amount of Centrelink data is held on hardware owned by private companies and leased to Centrelink - How does this ownership arrangement affect your security policies, especially concerning the issues of redundancy and disaster recovery?

Centrelink retains ownership, custody and control of its data whether or not the equipment is leased. All leased hardware is located on premises owned or leased by Centrelink. Both the physical and logical access to this hardware is protected and managed by Centrelink employees or contractors, policies, systems, and procedures.

In the event of a disaster Centrelink takes responsibility for the data held on IT hardware that it owns or leases from vendors similarly to paper based files. For example, after a fire destroyed the Centrelink Customer Service Centre in October 2002, the hard disk drives of all the IT hardware were retrieved and erased by Centrelink before being passed on to the insurer as was required in this case.

5. What action is Centrelink taking to guard against the potential problem of social engineering?

There will always be those willing to use whatever means possible to gain access to information that they are not entitled to. Centrelink has a number of systems, policies and procedures in place to help protect customer data from unauthorised access use and disclosure. Centrelink has an extensive privacy and security education program for all staff. Awareness programs and online screen based messages are a constant reminder to users of Centrelink systems of the need to be vigilant and protect customer data.

We understand that one of the way attackers using 'social engineering' work is via the telephone. This not only provides a shield for the attacker by protecting his or her identity, it also makes the job easier because the attacker can claim to be a particular person with more chances of getting away with it.

Some of the processes Centrelink has in place to guard against the problem of social engineering include:

- The security in depth principle has been implemented in both physical and logical security practices;
- Centrelink employees are trained in the 'ask, don't tell' principle and any suspicious calls are either terminated or referred/reported to management. A recent example of this occurred when a Customer Service Officer in a Centrelink Call Centre became suspicious of a particular caller and after terminating the call referred the matter to their team leader. The customer was contacted and they confirmed that they had not contacted Centrelink. Processes were put in place to ensure the security of the customer's record;
- Centrelink has an extensive outreach program. Area Privacy Officers and Security Contact Officers deliver training and outreach in relation to privacy and security;
- Visitors to Centrelink offices are escorted during their visit. Any person not wearing a Centrelink identification tag is challenged;
- Where fixed passwords are required, employees are required to choose 'strong' passwords and the employee must not reveal or share their password to any other person including systems administrators;
- Door passcodes, and passwords to any shared accounts are changed immediately when employees leave; and
- Hard drives of computers are erased when the computer is serviced by external vendors.

Centrelink continues to remain vigilant against such attacks.

6. What action is Centrelink taking to ensure the long-term archival integrity of its data?

I will answer the question in terms of 'structured data' (information contained within the customer database) and 'unstructured data' (email, spreadsheets, web content, images, video, voice etc).

In the last 12-18 months Centrelink has began a process of enabling structured data within the customer database to be identified for migration to the Archiving and Culling Engine. This work is ongoing and will enable potential long term retention in a common format to ensure access and retrieval. The format is consistent with standards being developed as part of the Victorian Electronic Records Strategy as well as work presently being undertaken by the National Archives of Australia.

Unstructured data will be addressed under the Centrelink 'IT Refresh' initiative. A component of IT Refresh is Content Management and this will enable both unstructured and structured data to have record keeping standards applied to information management and retention. Information will be retained and managed within a business activity context. This will result in information being retained according to National Archives requirements and prevent information being held longer than necessary or destroyed before its time. It will also result in being able to identify information that needs to be retained for long periods of time at the time of its creation. This will enable Centrelink to apply appropriate means for ensuring accessibility to only that information that requires this process.

I have enclosed an additional information package as was provided to the Committee on 31 March 2003.

Please contact Joan Savic from the Privacy and Information Access Team on 6212 0437 if you have any further questions.

Yours Sincerely,

Pat Fegan
National Manager
Business and Information Protection