facs making a difference

Supplementary 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 Department of Family and Community Services (FaCS) lodged its submission to the Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information in the Commonwealth on 24 December 2002. On 31 March 2003, Mr Tony Mee (Assistant Secretary – Business Information Solutions Branch) represented FaCS at the public hearing.

This supplementary submission provides departmental responses to additional questions raised by the Committee that were communicated in writing to the Department on 29 April 2003.

A. REPORTED BREACHES

1. A submission from the Office of the Federal Privacy Commissioner mentions an incident in June 2002 involving email addresses collected from a FaCS web site, *The Source*. The web site editor sent an unsolicited marketing message to these e-mail addresses on behalf of a third party.

- **Would you please provide the Committee with your comments on this issue?**

'The Source' is a web site administered by the Youth Bureau within FaCS. In 2002, the Department made use of email addresses that individuals had provided for the purposes of entering one competition, for the purposes of entering those email addresses into another competition on the same web site. It did so without authority. FaCS acknowledged that it had breached Information Privacy Principle 10.1 of the Privacy Act 1988. Once the matter was brought to the attention of the Department, the editor of the Source apologised to the handful of persons who complained to the Department. The Deputy Privacy Commissioner conducted a formal investigation into the incident, which included an audit of FaCS' IT systems.

The Deputy Privacy Commissioner wrote to the Department on 1 November 2002 noting the prompt action taken on this matter and his recommendations to the Department during the course of the investigation. He indicated that he was satisfied with the outcome of the actions taken by the Department and he would not take any further action under his investigation. A press release to that effect was released by the Office of the Federal Privacy Commissioner on 29 November 2002.

- **What has been done to prevent a recurrence of this sort of privacy breach?**

The Department conducted privacy awareness sessions with the staff involved in the incident. In addition FaCS:

- *Completed a privacy audit of its web sites.*
- *Amended its web site privacy statements to make them clearer.*
- *Destroyed the database with the web site visitor (email) addresses.*
- *Cleared up links so visitors can be sure which site they are supplying information to.*
- *Conducts regular privacy awareness training for staff in National and State offices.*
- *Appointed the Privacy Contact Officer to the Change Management Committee.*

2. The same submission also mentions an incident in November 2001 where the Child Support Agency sent e-mail to clients that inadvertently divulged 400 other e-mail addresses.

- **Would you please provide the Committee with your comments on this issue?**

A privacy breach occurred on 15 March 2002 to subscribers of the Child Support Agency (CSA) web site who had indicated that they wished to participate in CSA surveys. An e-mail was sent to the 392 subscribers inviting them to complete a survey. The addresses were not 'blind copied' and all recipients could view the mailing list.

The error was detected immediately and effort was made to recall the e-mail. Approximately 50 of the e-mails were not delivered because the addresses were invalid. An e-mail was sent to the recipients apologising for the error and requesting that they delete the communication. The original e-mail was then re-sent with 'blind copy' addresses.

The CSA contacted the Office of the Federal Privacy Commissioner (OFPC) advising them of the breach and the circumstances in which it took place. The OFPC recommended that the CSA:

- *Implement a checking procedure that staff must follow before sending multi-case e-mails;*
- *Allow only selected and authorised staff to send multi-case e-mails; and*
- *Provide specialist training to selected staff on privacy issues and procedures.*

The CSA has implemented all recommendations made by the OFPC.

B. ISSUES RAISED IN SUBMISSION

3. Your submission states that a consistent, whole of government approach is needed to equip non-government organisation (NGO) service providers to comply with stringent Government regulations for security and privacy.

- **What sort of whole of government approach do you envisage?**

Many NGO service providers provide services on behalf of several Commonwealth Government agencies. In most cases, each agency requires the service provider to enter into different contractual arrangements for the delivery of each service. Whilst high-level privacy requirements are largely consistent across the Commonwealth, information management arrangements (including security) and connection with each agency is not. This situation makes it difficult (and costly) for some service providers to do business with the Commonwealth.

FaCS is of the view that a whole of government approach to the compliance of stringent Government regulations for security and privacy are necessary. The use of electronic data and transfer is becoming more and more prevalent in the business environment, thus security and privacy requirements must become more consistent across Commonwealth agencies to allow service providers to interact effectively.

FaCS is currently developing a new on-line funding management system to manage the funding relationship with its several thousand NGO service providers. The system is being built to ensure it has capacity for consistent reporting, information collection and transfer across all service providers. We will be working with NGO service providers later in the project cycle to help streamline security and privacy requirements for them.

Given the scope and complexity of funding across many different programs, and the large number of NGO service providers we engage, FaCS is in a good position to help other agencies streamline their arrangements with NGO service providers for the greater whole of government good. We have already commenced discussion with another large Commonwealth agency that has expressed interest in the system.

FaCS also believes that the National Office for the Information Economy (NOIE) needs to take a greater role in coordinating this work across the Commonwealth.

- **What risks would such an approach seek to address?**

  - *The risk of a significant breach in security and privacy is greater where there are slightly different regulations for each agency making it confusing for service provider personnel to understand obligations imposed on them.*
  - *The risk that security and privacy regulations do not match the level of risk associated with delivery of functions increase as each agency develops their own standards.*
  - *The risk that the Commonwealth will not make use of advanced technologies to provide better services into the future is significant because the cost of compliance to use them by service providers is ultimately passed on to the Commonwealth.*
  - *The risk that the Commonwealth Government will not realise a true whole of government approach to managing service providers and managing information on a broad level is markedly increased. This leads to increased administrative cost and inhibits broad policy development across the Commonwealth to meet the requirements of citizens and communities in general.*

4. How does FaCS ensure the integrity, security and privacy of its data held by NGO service providers?

FaCS requires its many NGO service providers to comply with stringent security and privacy requirements. The primary mechanism used for ensuring this occurs is the use of clauses in legal contracts as a condition of receiving funding from FaCS to deliver programs and services on our behalf.

The specific clauses are:

FaCS Long Form Funding Agreement contains Clause 14 – Disclosure of Confidential Information (this clause is designed to protect the Commonwealth's confidential information) – "The Funding recipient must not disclose any confidential information to any third party without the prior written approval of the Commonwealth. The Commonwealth also agrees to protect the confidential information of the Funding Recipient. However, the Commonwealth has the right to disclose information to certain parties within Government and according to law".

FaCS Short Form and Long Form Funding Agreements contain Clauses 14 and 15 respectively – Protection of Personal Information (these clauses import the obligations of the Privacy Act (1988)). "If the Funding Recipient breaches the obligations set out in the Privacy Act, it will have committed a breach of the Agreement".

Annexure A of the FaCS Long Form Funding Agreement – Confidentiality Deed Poll (under Clause 14 of the Agreement the Commonwealth has the right to ask for a Confidentiality Deed Poll). The Confidentiality Deed Poll mirrors the obligations set out in clauses 14 and 15 of the Agreement and expands the Funding Recipient (or third party) obligations relating to confidential and personal information).

Program areas within FaCS are responsible for ensuring NGO service provider compliance to funding agreements. Program management and service delivery business processes used by program areas are regularly subject to internal audit activity to ensure effectiveness.

5. Your submission states that it is difficult to manage stringent security requirements at the same time as taking a flexible approach to work and service delivery.

- **How can the problem of achieving balance between security and flexibility be resolved?**

The balance between security and flexibility is a complex one. On one hand the Commonwealth is wanting to provide greater flexibility in doing business with others by taking advantage of ever sophisticated emerging technologies, whilst on another, unnecessarily complex and stringent security requirements are imposed making it difficult for new technologies to be utilised. This is in part due to the current state of transition within government to the use of electronic service delivery.

At present, to move to a more protected or higher classified network, FaCS must use Defence Signals Directorate (DSD) endorsed products. We are required to investigate a large range of individual DSD endorsed products and attempt to integrate their benefits to build a tailor made approach. This process is time consuming, not just for FaCS, but also for every other agency that must follow the same process. A more proactive and integrated way to endorsing products using a scenario-based approach of Commonwealth requirements would be helpful.

C. ARCHIVAL INTEGRITY

6. Your submission states that there needs to be a whole of government strategy to identify data sources that need to be preserved over long periods of time, and to ensure that such data remains accessible despite changes in technology.

- **Would you expand on your Department's view of the problems associated with the long-term storage of electronic data?**

As government agencies move increasingly towards capturing and retaining information in an electronic format, the volume and size of that data and the importance of that data will continue to grow.

Each agency takes responsibility for the collection, maintenance and storage of its official information. The risk with this approach is that agencies identify what data sources need to be preserved over time and the mechanisms to ensure that they remain accessible. These decisions are generally made within current funding constraints and the existing business environment.

In general, there is little consideration given to the retention and access requirements of government over the long term.

Retaining information in an electronic format raises many questions:

- *Will the information be important in 20 years time?*
- *How will we manage it?*
- *How will we retain it?*
- *How will we classify that information over long periods of time; and*
- *How will we be able to access it and use it across government to support whole of government objectives?*

A whole-of-government strategy to address these issues is critical.

- **Do you have any suggestions which could be applied in the development of a whole of government approach?**

    - *The National Office for the Information Economy (NOIE) should play a role in raising awareness of this important issue to agencies, especially under Information and Communication Technology (ICT) outsourcing arrangements.*
    - *The identification and preservation of important information should be a standard contractual requirement.*
    - *Important long-term data should be identified and resources directed at the preservation of data, rather than trying to manage all data the same way.*
    - *Systems should be put in place for identifying all important and vital information in organizations.*
    - *Record keeping and preservation requirements should be built into standard information application system development methodologies.*
    - *Retention requirements for data to be identified at the system design stage and appropriate strategies in place to ensure preservation and access to data for as long as access is needed.*
    - *Data to be retained for long periods should be stored and described using data storage and software standards that have a long shelf life eg XML.*
    - *Strategies to migrate important data across changes in technology and software are required – resources need to be allocated.*
    - *Encryption and PKI need to be managed to allow public access under the Archive Act to data that has been in existence for 30 years.*

- **What action is FaCS taking to ensure the long-term archival integrity of its data?**

    - *Identifying standards that have a long 'shelf life'.*
    - *Implementing an electronic document management system that provides appropriate management of data for the identified life of that data.*
    - *Developing a metadata framework to assist in maintaining the integrity of data.*
    - *Identifying data sources where the long-term archival integrity of those sources is at risk and migrating that data to a non-propriety format e.g. Guide to the Act.*

D. SOCIAL ENGINEERING

7. Social engineering is the use of deception, influence and persuasion to overcome security measures. This is a potential risk to the privacy and security of electronic data, but is not mentioned in the FaCS submission.

- **What action is FaCS taking to guard against this potential problem?**

FaCS takes this issue very seriously. The primary mitigation strategy used for reducing the risk of social engineering is to educate staff. Regular information articles are placed within weekly all-staff newsletters and the monthly FaCS Information and Technology Report. Articles provide staff with information about what social engineering means, how social engineering has been used within organizations to overcome security measures and what to look out for. We also have a security contact officer that staff can contact if they wish to discuss social engineering.

The education strategy is complemented by a number of broader FaCS policies in place to protect the privacy and security of electronic data. They include:

- ***General IT Security Considerations*** *- stipulates that no devices or other equipment are to be connected to the FaCS network without approval and that workstations connected to the FaCS network shall remain sealed to prevent surreptitious access.*
- ***E-mail Security*** *- states the limitations imposed by FaCS for using e-mail to transmit classified Commonwealth information. It is FaCS policy that this information is not to be sent to any external addresses, as they are not secure.*
- ***IT Password Security*** *- passwords are not to be shared and that passwords are to be in a DSD format.*
- ***Workstation Security*** *- states that users are to logoff from the system if they are away from their workstation for periods exceeding one hour.*
- ***Disposal and Destruction of Removable Magnetic Media containing Commonwealth Information*** *- all storage media containing Commonwealth information will be disposed of in an ASIO approved manner.*
- ***Records Management*** *- contains information on how to security classify information.*
- ***Security Clearances*** *- all officers who have access to information security classified at the PROTECTED level or higher are to have an appropriate security clearance.*

E. DISASTER RECOVERY

8. A potential threat to the integrity of the Commonwealth's electronic data is physical disruption caused by an earthquake or fire.

- **Would you outline for the Committee your disaster recovery plan?**

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, an IT Disaster Recovery Plan has been implemented as part of a wider Business Continuity Management Project.

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 disaster recovery documentation and other risks to the recovery process. These recommendations are currently being addressed.

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