QUESTION TAKEN ON NOTICE

ADDITIONAL ESTIMATES HEARING: 13 FEBRUARY 2012

IMMIGRATION AND CITIZENSHIP PORTFOLIO

(AE12/0273) Program 3.1: Border Management

Senator Cash asked:

What guarantees or auditing measures exist to ensure the confidentiality of applicants and applications and privacy protection of their information handled by a Service Delivery Partner (SDP)?

Answer:

Ensuring the confidentiality of applicants and applications is the most crucial feature of an arrangement with the SDP and there are a number of controls in existence to ensure compliance:

- The Department of Immigration and Citizenship (DIAC) has clearly defined privacy and confidentiality requirements of an SDP during contractual negotiations and in the final Deed of Agreement to ensure the SDP implements organisational strategies and systems to ensure staff understanding of and compliance with privacy requirements.

- DIAC aligns privacy and confidentiality requirements in the Deed of Agreement with clear standards and performance expectations to ensure that requirements are clear and consistent. Specifically, documented in the Deed of Agreement an SDP must meet the same level of privacy as required under the Australian Commonwealth Privacy Act 1988 and the Information Privacy Principles contained within that legislation.

- DIAC ensures appropriate training in privacy provisions and professional conduct requirements is included in SDP implementation phase and that sanctions are clearly communicated to and understood by SDP managers and staff.

- <u>IT and Data Security Systems</u>
  The SDP is contractually required to establish and maintain safeguards against the destruction, loss or alteration of DIAC Data in its possession.

  The SDP is to comply with the reasonable guidelines and instructions on the storage, security and privacy of DIAC Data which includes guidelines on the type of, and the length of time that, data that can be stored on the SDP's systems.

Some data security measures include:

- basic data from the application is kept for tracking purposes until the visa is finalised and then purged;
- biometric data is not stored by the SDP as it is transmitted immediately to DIAC upon collection;
- all users are required to use a unique identification logon and password to access the Technical Infrastructure. The use of access control and file permissions must be set to restrict users to data on a "need to know" basis.
- auditing of user access must be provided. User activity must be logged, archived for a minimum of six (6) months and centrally monitored using industry best practice. Applicant Data must be encrypted to FIPS140-2 standard;
- all users are required to change their passwords to access the Technical Infrastructure at least every three (3) months (or such other period agreed by the Parties);
- users' screens must lock after a period of inactivity; and
- disposal of faulty or redundant magnetic media (tapes, hard drives, etc.) must be carried out securely.