(By Hand)

Our Ref: PCO/1/10/2
Your Ref: CB2/BC/6/01

21 February 2003

Mrs. Sharon TONG
Clerk to Bills Committee
Legislative Council
3/F Citibank Tower
3 Garden Road
Hong Kong

Dear Mrs. Tong,

**Bills Committee on**
**Registration of Persons (Amendment) Bill 2001**
**Privacy Compliance Audit**

Thank you for your letter dated 12 February 2003. We are pleased to provide additional information on the captioned subject for further deliberations by Members of the Bills Committee.

**Discussions between the Administration and PCO**

The Administration has been discussing with the PCO on making necessary arrangements for a privacy compliance audit to be conducted 12 months after the implementation of the Smart Identity Card System ("SMARTICS"). Our present understanding is that the Immigration Department will draw up a code of practice relating to SMARTICS after the completion of the fourth Privacy Impact Assessment study which is currently planned to be undertaken about 3 months after the system cut-over date. The code will set the ground rules on the collection, use and access of smart identity card data and make provisions for the conduct and frequency of privacy compliance audits. If required, the Privacy Commissioner may approve the code pursuant to section 12 of the Personal Data (Privacy) Ordinance.

It is our intention to incorporate details of the agreed arrangements in a memorandum of understanding to be drawn up between the parties. This will include the terms of reference, the duration, the provision of resources and other relevant matters pertinent to the conduct of the privacy compliance audit.

**The SMARTICS audit approach**

The code of practice, when approved, will form the benchmark for which the compliance of SMARTICS will be assessed and audited. The audit will comprise of the following key components:

a) **The audit team**. Prior to the conduct of the audit, the PCO will agree with the Immigration Department on the scope of the audit. On the basis of our present understanding, it is envisaged that the audit will take about 4 elapsed months to complete. The provisional requirement is have a team that would encompass a mixed set of skills in auditing, information process management and the application of data protection principles.

b) **The audit process**. A principal activity of the audit is to obtain evidence to enable the audit team to assess the extent to which the information management processes of SMARTICS are implemented in accordance with stated privacy policies, data protection principles, codes of practice or other regulatory requirements. Another key activity is to verify that all privacy issues identified in the Privacy Impact Assessment studies are properly addressed in the delivery of SMARTICS, that safeguards to enhance privacy protection are implemented as promised and that control mechanisms are put in place to ensure on-going privacy compliance. If necessary, confirmatory audit testing may be carried out by means of random sampling of data held in SMARTICS. It is also intended to make use of the PCO's privacy compliance self-assessment (Privacy.SAFE) tool-kit, with suitable adaptation of the SMARTICS environment, as the guiding audit field-work procedures. A copy of the privacy compliance self-assessment tool-kit is enclosed with this letter.

c) **Reporting**. The results of the audit and any recommendations arising from the audit will be presented in the form of a draft report which is submitted to the Administration for its comments and response. The draft report and the Administration's responses on matters addressed in the draft report will then form the basis of the final audit report. It is our understanding that the Administration will provide a copy of the audit report to the Legislative Council for Members' reference.

I trust the Chairman and Members of the Bills Committee will find the above information helpful in their further deliberations.

Yours sincerely,

(Raymond Tang)
Privacy Commissioner for Personal Data

Encl.