For information on
7 December 2010

Legislative Council Panel on Security

Privacy Compliance Assessment Report
On Smart Identity Card System (SMARTICS)

Purpose

This paper reports to Members the recommendations made by the Office of the Privacy Commissioner for Personal Data (PCPD) in the Privacy Compliance Assessment Report on the Smart Identity Card System (SMARTICS) (please refer to LegCo Paper No. CB(2)2137/09-10(01) issued by the Legislative Council (LegCo) Secretariat on 2 August 2010 for the full report), and the follow up actions taken by the Immigration Department (ImmD).

Background

2. The Smart Identity Card was introduced in 2003. In drawing up the relevant data protection measures, ImmD has all along sought the views of the PCPD and has strictly adhered to the relevant legal requirements. ImmD also put in place all necessary measures to fully safeguard personal data privacy.

3. Throughout the various stages in the development and implementation of SMARTICS from 2000 to 2004, ImmD commissioned privacy consultants to conduct four privacy impact assessments (PIAs) of the system. ImmD had fully implemented the measures recommended by the consultants and incorporated necessary privacy protection measures in SMARTICS computer system. Thereafter, ImmD had further conducted two privacy compliance self-assessments in 2005 and 2008 respectively to ensure that the data protection requirements be fully complied with.

Findings of the Privacy Compliance Assessment Report

4. To further ensure that the operation workflow and processes of SMARTICS could fully safeguard the protection of personal data, ImmD invited the PCPD to conduct a Privacy Compliance Assessment (PCA) in an independent and professional manner. The assessment was conducted from July to November 2009, and the PCA Report was presented by PCPD on 30 July 2010. The report had been submitted to the LegCo Panel on Security for reference and the Report has also been uploaded onto ImmD website for public access.

5. Overall, PCPD is satisfied that ImmD has put in place protection measures, and confirmed that the operation workflow and processes of SMARTICS has complied with the relevant requirements of the Personal Data (Privacy) Ordinance. PCPD found that the ImmD has put in place appropriate policies and guidance in handling personal data. The PCA Report considers that ImmD has followed the principle of protection of privacy in its system design and has conducted PIAs effectively throughout the planning of the SMARTICS. Also, the PCA Report noted that ImmD has drawn up the "Information Technology Security Policy for ImmD" to ensure data confidentiality, and has drawn up the "Information Technology Security Guidelines for ImmD" to elaborate the relevant responsibilities and procedures. PCPD is generally satisfied that these documents can cover the confidentiality and integrity aspects in data security.

6. In addition, the PCA Report recognizes that the use of smart identity card data has complied with the "Statement of Purpose" for the collection of personal data, and has complied with the requirements of the relevant legislation. The PCA Report is generally satisfied with the degree of transparency of ImmD in making available to the public its Privacy Policy, and in enabling members of the public to access personal data. The PCA Report also noted that ImmD has published a "Statement of Privacy Policy and Practices" booklet, which publicises the privacy policy of ImmD and the categories of personal data held by ImmD.

Recommendations of the Privacy Compliance Assessment Report

7. Meanwhile, the PCA Report has made 16 recommendations on enhancing the various procedures relating to the handling of personal data privacy by ImmD, such as amending the identity card application form to specify the consequences for failing to supply personal data, enabling more staff to participate in training programmes relating to privacy protection, improving the sound insulation of the registration booths in the Registration of Persons Office and adjusting the position of self-service kiosk to enhance privacy protection. All in all, ImmD has implemented 14 of the recommendations, and will implement the remaining two by the first quarter next year. The implementation of the 16 recommendations is set out at Annex.

8. Members are invited to note the content of this paper.

Security Bureau
November 2010

Annex

Office of the Privacy Commissioner for Personal Data

Privacy Compliance Assessment Report

Recommendations and Follow up Actions

Recommendation	Contents	Follow up Actions
1	Amend the SMARTICS Security Guidelines to define the security requirements for data and handling procedures, and conduct related training programmes.	Implemented.
2	Clearly set out the updating procedures of SMARTICS Manual Procedures.	Implemented
3	Revise the identity card application form to specify clearly the consequences for failing to supply personal data.	Implemented.
4	Provide more specific review guidelines to reviewers to ensure that all reviewers are familiar with the checking procedures.	ImmD is now reviewing the audit guidelines in use, and will issue more specific guidelines to enhance the awareness of reviewers on the checking procedures. The relevant works will be completed by February 2011.

5	Conduct training programmes to raise staff awareness on the guidelines on change of password.	Implemented; ImmD has provided training to staff to enhance their understanding on the relevant guidelines.
6	Conduct training programmes to ensure that staff members responsible for handling data access and correction requests are familiar with the relevant guidelines in the Personal Data (Privacy) Ordinance.	Implemented; ImmD has conducted two specific training sessions to staff members responsible for handling data access and correction requests, and training sessions will be conducted regularly in the future.
7	Enable more staff to participate in training relating to privacy protection.	Implemented; 14 training sessions has been conducted, and training sessions will be conducted regularly in the future.
8	Speed up the reporting of the results of the Privacy Compliance Self-Assessment Exercises.	Implemented; ImmD will issue the report upon receipt when conducting Self-Assessment Exercises in future.
9	Enhance the practice of the Confidential Records Unit in providing smart identity card data to other Government departments.	ImmD is enhancing its system so that the Unit would only print out the specific data required. The relevant works will be completed by February 2011.
10	Ensure encryption of the backup tapes, and the proper movement of the backup tapes.	Implemented; ImmD has revised the software for monitoring the location of the backup tapes to ensure its accuracy.
11	Improve the sound insulation of the registration booths in the Registration of Persons Office to ensure privacy protection.	Implemented; measures taken include installation of acrylic panel and rearranging the layout of the registration booths.

12	Adjust the position of self-service kiosk to prevent smart identity card data from being viewed by other parties.	Implemented; measures taken include improving the arrangement of self-service kiosks (changed to linear arrangement), installing screen protectors for the computer monitors at the self-service kiosks, and installing partitions between kiosks.
13	ImmD had set limits to the data content that are accessible by staff of various rank / post, which is set out in a "Security Matrix". ImmD should assign version number for the "Security Matrix" and state clearly the distribution mechanism of the Matrix, and ensure that the updated version is distributed to and used by all relevant parties.	Implemented.
14	Review the procedure on controlling the access of information by staff members who are on leave.	Implemented; ImmD had revised the relevant guidelines so that staff members who are on leave for more than two weeks would not have access to the data. Also, staff members need to obtain permission from the section head before they can return to the office during the leave period.

15	Ensure staff members' compliance with procedures in relation to the returning, recording and checking of identity card captured by self-serving kiosks.	Implemented; ImmD has enhanced trainings and guidance to staff, and reminded them to strictly adhere to the established procedures and practices in handling smart identity cards captured by self-serving kiosks.
16	To align the expiry period for changing password to every three months.	Implemented; relevant guidelines has been revised to require staff members to change their passwords at least once every three months under the enhanced requirements of the SMARTICS.