立法會
Legislative Council

LC Paper No. CB(2)277/12-13(05)

Ref : CB2/PL/SE

Panel on Security

Background brief prepared by the Legislative Council Secretariat for the meeting on 4 December 2012

Information Systems Strategy and Immigration Control System of the Immigration Department

Purpose

This paper provides background information relating to the Information Systems Strategy ("ISS") and automated passenger clearance system ("e-Channel") of the Immigration Department ("ImmD") and summarizes the discussions of the Panel on Security ("the Panel") on the subject.

Background

2. Since the 1980s, ImmD has been adopting information technology ("IT") to support its day-to-day operations. According to the Administration, the use of IT is critical for ImmD in coping with the dynamic business environment with growing service demands from over seven million population and much increased volume of visitors. The passenger traffic handled by ImmD increased by 70% from 142 million in 2000 to 241 million in 2010. The number of visa applications processed also increased from 123 300 to 270 700 over the same period, representing an increase of 120%.

3. ImmD formulated its first ISS ("ISS-1") in 1991, followed by the second ISS ("ISS-2") in 1999. According to the Administration, the IT application systems of ImmD are used for supporting various business areas, such as immigration control, personal documentation as well as visa control and enforcement.

4. After the full implementation of ISS-2 programmes, ImmD commissioned external consultants to conduct the third ISS ("ISS-3") review, which was completed in September 2010. The ISS-3 blueprint encompasses eight strategic IT projects in a structured programme from 2012-2013 to 2018-2019. The eight ISS-3 projects are:

(a) Next Generation Information Technology Infrastructure ("ITI");

(b) Immigration Control System ("ICONS");

(c) Visa Automation System;

(d) Assistance to Hong Kong Unit, Births, Deaths & Marriage, Right Of Abode ("ROA") Decision Support System;

(e) Next Generation Electronic Passport System;

(f) Next Generation Smart Identity Card System;

(g) Enforcement Case Processing System; and

(h) Human Resources Management System.

5. According to the Administration, the eight ISS-3 projects are inter-related and essential to ImmD's mission-critical operations. Implementation of ISS-3 would generate department-wide service improvement opportunities including further extension of self-service immigration clearance at control points. The Finance Committee approved at its meeting on 9 December 2011 a new commitment of $862,202,000 for the implementation of Information Technology Infrastructure and acquisition of data centre services for ImmD.

Immigration Control System

6. ICONS is one of the eight projects under ISS-3. In June 2012, the Administration informed the Panel that ImmD was conducting a feasibility study on ICONS. The scope of the study covered, among other areas, setting up an effective platform in support of extension of e-Channels and the feasibility of deploying facial recognition technology to further enhance e-Channel security and detection of forgeries. The study was expected to be completed before the third quarter of 2012.

Deliberations of the Panel

7. The implementation of ISS and issues relating to e-Channels were discussed at various Panel meetings. The deliberations are summarized in the following paragraphs.

Information Systems Strategy

8. Information was sought on the measures adopted to prevent loss of data arising from failure of the new system and restrictions on access of the personnel of ImmD to the electronic records. According to the Administration, the new system would feature duplex servers and a resilience centre located on the other side of the harbour. The network would be carefully designed to ensure system security and data integrity. There would be restrictions on access to the computer system and electronic records according to the nature of work of the respective posts.

9. Concerns were raised over the integrity of the data with the implementation of the new system and possible difficulties in finding records of ImmD relating to ROA. According to the Administration, records would be stored in the form of electronic images under the new system to facilitate retrieval. It was a practice of ImmD to assign a reference number to each application. In designing the new system, ImmD would consider whether a check-list of documents collected from an applicant could be produced by the system for the reference of the applicant. ImmD would answer all enquiries made through electronic mail ("e-mail").

10. There was a suggestion that besides acknowledging receipt of a document, ImmD should also confirm that the document received had been stored in its electronic system. According to the Administration, all documents collected from an applicant would be converted into digital format and stored in the new system, and ImmD would acknowledge receipt of the documents. After an application had been processed, the applicant would be notified of the decision and necessary information would be retained in the system. The new system could incorporate the function of acknowledging receipt of document submitted, if necessary.

11. Members had sought information on the circumstances under which an incoming e-mail would be permanently stored in the new system of ImmD, its legal status under local legislation.

12. According to the Administration, e-mails sent to ImmD would be captured and stored electronically under the proposed system with acknowledgement receipts sent to senders. The Electronic Transactions Ordinance (Cap. 553) provided a general legal basis for the acceptance of electronic submissions and digital signature to satisfy rule of law requirements for information in writing and signature etc., including immigration-related matters. The length of period in which a piece of electronically stored information was to be retained by ImmD under the present paper/microfilm records system would depend on the nature and possible use of such information. In principle, a piece of electronically stored information would be retained in the system so long as their retrieval might be required for the processing of an application and the taking of follow-up and other actions as might be envisaged. For instance, those related to ROA were permanently kept by ImmD.

Automated passenger clearance system

13. Members noted that the e-Channels deployed fingerprint verification technology for authentication of a person's identity. Concern was raised as to whether there would be measures against the use of false fingers or artificial fingerprints at e-Channels. According to the Administration, the fingerprint scanner was capable of detecting the liveliness of a finger through the detection of electric current and blood flow in the finger.

14. Concern was raised about the security of the e-Channels following a press report in January 2012 on the successful attempts by a reporter to pass through e-Channel by using a fake fingerprint membrane made of a kind of material available for sale on the internet. There was a view that ImmD and the system contractor had not conducted the regular inspection and maintenance properly and had not kept themselves abreast of the updated technology. Members expressed concern as to whether there was any record on the malfunction of the e-Channels which had caused other successful gate-crashing cases since its introduction in 2004 and whether the malfunction of an e-Channel would be identifed. In addition, queries were raised about the accuracy of the immigration records. Members suggested that the frequency of the inspection of e-Channels should be increased, and sought information on the maintenance of the e-Channel concerned.

15. According to the Administration, it was the first time that a visitor had been able to pass through an e-Channel by the use of a fake fingerprint membrane. Regular inspection and maintenance of each e-Channel were done

every six months. Additional inspection of e-Channels would be conducted as necessary. After the incident, the e-Channel concerned was closed down and the fingerprint scanner of that e-Channel was dismantled and returned to the manufacturer for detailed inspection. While awaiting a comprehensive report on the investigation of the incident, ImmD had conducted thorough testing for all e-Channels by making use of the fingerprint model provided by the reporter and other fake fingerprints. It was found that all other e-Channels were secure and reliable, and the immigration records of visitors were accurate.

16. Concern was also raised as to whether there were cases involving the use of forged smart identity cards by Hong Kong residents in an attempt to perform self-service immigration clearance through e-Channels. According to the Administration, between the introduction of the e-Channel service in December 2004 and February 2010, ImmD had never discovered any cases of Hong Kong residents using forged identity cards to pass through the e-Channels successfully.

17. Members noted that some people could not use their smart identity cards for automated immigration clearance through the e-Channels due to fingerprint recognition problem. Information was sought on the measures to be introduced to reduce failure in fingerprint verification.

18. According to the Administration, some people with blurred fingerprints might have difficulty in using e-Channels. This was because the fingerprint scanner used on the spot might not be able to capture a good fingerprint image. In some circumstances, for example, when the weather was dry, the fingerprint identification problem was more distinct. Statistics showed that less than 1% of smart identity card holders had such a problem.

19. Clarification was sought on whether the process for immigration clearance would be prolonged with the application of both fingerprint verification and facial recognition technologies. The Administration advised that facial recognition technology had been well developed over the years and its accuracy was comparable to that of fingerprint verification. The application of facial recognition technology would strengthen the security of the e-Channel system, given the two levels of security. In view of the global development of electronic document and self-service immigration clearance as well as the inclusion of an electronic or digital photo in the electronic travel document as required by various immigration authorities in other countries or regions, the adoption of a second biometrics was being studied. These included the synchronization of the application of both fingerprint and facial recognition technologies and the additional security in the identification process. The

Administration further advised that the processing time would not be lengthened.

Relevant papers

20. A list of the relevant papers on the Legislative Council website is in the **Appendix**.

Council Business Division 2
Legislative Council Secretariat
30 November 2012

Appendix

Relevant papers on the Information Systems Strategy and Immigration Control System of the Immigration Department

Committee	Date of meeting	Paper
Panel on Security	1.11.2001 (Item III)	Agenda Minutes
Panel on Security	6.12.2001 (Item III)	Agenda Minutes
Finance Committee	11.1.2002	Minutes FCR(2001-02)54
Panel on Security	5.12.2002 (Item III)	Agenda Minutes
Finance Committee	24.1.2003	Minutes FCR(2002-03)51
Panel on Security	16.3.2004 (Item IV)	Agenda Minutes
Finance Committee	14.5.2004	Minutes FCR(2004-05)10
Panel on Security	7.12.2004 (Item IV)	Agenda Minutes
Panel on Security	6.1.2009 (Items IV and V)	Agenda Minutes
Panel on Security	2.2.2010 (Item IV)	Agenda Minutes
Panel on Security	1.6.2010 (Item IV)	Agenda Minutes

Committee	Date of meeting	Paper
Finance Committee	9.12.2011	Minutes FCR(2011-12)56
Panel on Security	13.3.2012 (Item IV)	Agenda Minutes

Council Business Division 2
Legislative Council Secretariat
30 November 2012