For information LC Paper No. CB(2)905/03-04(01)

Panel on Security of the Legislative Council

Hong Kong Special Administrative Region (HKSAR) Identity Card Project: Progress Report

INTRODUCTION

This paper updates Members on the latest development of the HKSAR Identity (ID) Card Project.

ISSUE OF NEW IDENTITY CARDS

2. The new procedure for registration of persons under the Smart Identity Card System (SMARTICS) was implemented on 23 June 2003. Smart ID cards are issued to the following groups of persons-

i) newly arrived immigrants;

ii) children eligible for juvenile ID cards upon reaching the age of 11;

iii) young persons eligible for adult ID cards upon reaching the age of 18;

iv) persons whose ID cards have been lost, destroyed, damaged or defaced;

v) persons who request to amend their particulars printed on their existing ID cards; and

vi) holders of valid identity cards who are invited to apply for new ID Cards during the territory-wide ID card replacement exercise.

3. The new procedure has been working smoothly except during the first two days when a small number of teething problems were quickly rectified. As at 15 December 2003, a total of 510,217 smart ID cards were issued.

TERRITORY-WIDE ID CARD REPLACEMENT EXERCISE

4. The first cycle of the territory-wide ID card replacement exercise commenced on 18 August 2003 and has been making good progress. It covers members of the Immigration Service, police officers, labour inspectors and Hong Kong residents born in 1964 to 1969[1]. The Chief Executive, members of the Executive Council, members of the Legislative Council and principal officials appointed pursuant to a nomination under Article 48(5) of the Basic Law may also apply to replace their ID cards during the first phase of the exercise. Alternatively, they may wait until the time specified for residents in their age groups.

5. The second cycle of the replacement exercise, covering holders of ID cards born in 1958 to 1963, will commence on 15 March 2004 and end on 25 September 2004. An order by the Secretary for Security stipulating the details of this cycle was laid before the Legislative Council for negative vetting on 17 December 2003. A further order stipulating the details of the third cycle will be laid before the Legislative Council for negative vetting in May 2004.

PROCUREMENT OF ADDITIONAL BLANK SMART CARDS

6. The tender for procuring another 4.7 million blank smart ID cards was issued on 4 July 2003 and closed on 15 August 2003. Following approval by the Central Tender Board of the recommendation of the Inter-departmental Assessment Panel, the new contract was awarded on 2 November 2003. The first batch of 800,000 smart cards will be delivered in April 2004.

THE THIRD PRIVACY IMPACT ASSESSMENT

7. The Consultant has completed the third privacy impact assessment (PIA) and submitted a report to the Immigration Department (ImmD) (copies of the report have been forwarded to the Clerk to the Security Panel). The Consultant finds, among others, that ImmD is privacy conscious and has a strong commitment to addressing any privacy issues and concerns arising from the SMARTICS project. The Consultant's

[1] Holders of ID cards who were born in 1968 or 1969 should apply for smart ID cards from 15 September 2003 to 15 November 2003, followed by those born in 1966 or 1967 who should make their applications from 17 November 2003 to 10 January 2004, and those born in 1964 or 1965 who should make their applications from 12 January to 13 March 2004.

report provides a comprehensive assessment of Government's response to the privacy issues raised in the second PIA, acknowledging that these issues have been addressed by ImmD in the design of SMARTICS which incorporates the privacy enhancement and protection measures recommended. The Report also confirms that the manual procedures as well as the system controls and functionalities developed for the production environment are privacy positive. The Consultant has, nevertheless, also identified a few specific areas in respect of manual procedures, system controls and access security, and disclosure of personal data where improvements are possible. The Consultant has also formulated corresponding proposals which will assist ImmD to further enhance the privacy of data in these areas.

8. A summary of the Consultant's findings and recommendations, as well as the Administration's responses, are set out at **Annex**. We have discussed them with the Privacy Commissioner for Personal Data whose views, where applicable, are also set out at Annex. It is noteworthy that ImmD is already taking measures to comply with the Consultant's recommendations, and have achieved compliance in some cases.

9. Actions to prepare for the fourth PIA are in train. We expect to commence it around January 2004. Its outcome will assist in the compilation of a Code of Practice (COP) governing the collection, storage, access, use and disclosure of ROP data. The COP would, in turn, provide the basis for the privacy compliance audit scheduled to be conducted further down the road.

Security Bureau
6 January 2004

Annex

Third Privacy Impact Assessment
Summary of Recommendations

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
1.	Procedures over handling of key privacy related audit logs generated by the SMARTICS should be further refined. (Manual Procedures)	The SMARTICS has been designed with many logging functions to track the usage of the system and to report any exceptional transactions/actions performed by users. Certain audit logs produced by the SMARTICS are considered privacy positive if used effectively. We understand that there have been long-established high-level policies and procedures within the ImmD regarding the retention, checking and disposal of different audit logs. These general policies and the related procedures will need to be further reviewed and refined with the privacy requirements surrounding the SMARTICS. Under the SMARTICS and depending on the type of audit log, different ImmD officers will be assigned the responsibility to review and respond to log events. However, detailed and formalised procedures over the review of these logs have not yet been developed at the time of the 3rd PIA. Such procedures will help to ensure that respective logs will be used effectively as a privacy enhancing measure. • ImmD should develop detailed procedures on how key privacy related audit logs that would be used as privacy protection measures should be reviewed. Key steps would include • The Principal Immigration Officer (Information Systems) Production ("PIO(IS)P") is to oversee the identification of key privacy related audit logs with reference to the overall privacy compliance framework. • Detailed procedures should be developed on the review of those key privacy related audit logs that could be used as privacy	--	Will comply through the following measures : - to incorporate a chapter on 'checking/safe-keeping, retention and disposal of computer records' in every volume of the manual procedures (already implemented); - to strengthen the privacy protection measures (we are now preparing a new chapter on the checking, retention and safekeeping of privacy related audit logs); and - to conduct a review to identify the key privacy related audit logs (after that, the relevant procedure will be drawn up in the manner suggested by the PIA consultant).

Item	Issues	3rd PIA Consultant’s Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government’s Response/ Way Forward
		protection measures. The procedures should, among others, state clearly who is responsible for reviewing the logs, what is being reviewed, how frequent is the review and what are the follow-up procedures if exceptions are noted. Formal channels should be established to facilitate escalation of potential or genuine privacy issues identified by section management from reviewing the logs to the PIO(IS)P and/or his team. These audit logs and the evidence of review by responsible section management should be kept properly to facilitate future privacy compliance audits.		
2.	Formal procedures should be established to review user access rights periodically to ensure that they are appropriate and not excessive. (Manual Procedures)	We understand that maintenance of user access rights in the SMARTICS will mainly follow the existing procedures of the ImmD. The SMARTICS controller is responsible for assignment and change of user access rights by using the function “Regular/Temporary User Privilege Assignment”. Based on the “Proposed User Profile” document as at 31 May 2003, this function is also granted to all Chief Immigration Officer (“CIO”) and Senior Immigration Officer (“SIO”) of different sections/offices within the ImmD that require access to the SMARTICS. This function is intended to be used by the CIO/SIO under special situations and they can only grant the access rights they possess to the users within their respective sections. At the time of the 3rd PIA, a comprehensive approach and procedures in relation to monitoring user privilege assignment was in the process of being developed. User section management is ultimately responsible for ensuring that access rights are appropriately granted to SMARTICS users within their own jurisdictions. If there are inadequate monitoring procedures over the user maintenance activities, excessive access rights may be granted to SMARTICS users. As a privacy positive measure, ImmD should develop formal procedures to ensure access rights are granted appropriately to SMARTICS users and are not excessive in relation to the users’ job roles. The procedures should include the following:	--	Will comply through the following measures: - to include a chapter on the checking, safe-keeping, retention and disposal of the audit trail report and the user profile maintenance report in the Manual Procedures (designated officers in each section were assigned to check the reports to ensure the accuracy and appropriateness — already implemented); - to draw up procedures: • to ensure the access rights are granted appropriately in relation to the users’ job role; • for user sections to ensure user access rights are commensurate with

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		• The CIO/SIO of each section/office should perform regular review on the access rights granted to the respective section users via the SMARTICS user management enquiry function to ensure users' access is commensurate with their current job roles. For example, users may have changed their roles but their access rights may have not been changed accordingly or users may have been granted additional access rights temporarily but the additional access rights have not been removed when it is no longer required. • The SMARTICS controller should review on a daily basis the audit log report on User Maintenance Any abnormal activities identified from this review should be investigated and followed up with the respective section's CIO/SIO, if necessary.		their current job roles; and • to conduct daily review on the audit trail report to identify any abnormal user maintenance activities.
3.	The Code of Practice on ROP data should be developed as soon as practicable after the 4th PIA. (Disclosure and Policies)	The Code of Practice ("COP") on ROP data is designed to provide practical guidance to individuals concerned in the handling of personal data with respect to the requirements of the PD(P)O. From the initiation of the SMARTICS project to the operations of the SMARTICS, a number of parties are involved in the handling of personal data, including internal ImmD staff, contractors of the SMARTICS and other authorised users. The COP should govern the behaviour of all these parties and individuals during the course of their work wherever personal data is involved. It should also assist them to understand clearly what are expected from them in terms of PD(P)O's requirements. At the time of the 3rd PIA, the ImmD has begun to develop a framework for the COP. We recommend that the COP be completed and made available to all individuals concerned as soon as practicable, possibly shortly after the completion of the 4th PIA so that any issues and recommendations from the 4th PIA can be addressed. The Principal Immigration Officer (Information Systems) Production, being the designated ImmD officer to monitor and oversee compliance with the PD(P)O, and/or his team should also be involved in the development of the COP to ensure all privacy principles are	It is noted that in the 3rd PIA report, the data privacy consultant has put forth some constructive suggestions on the coverage of the Code of Practice and how the Code should be developed. PCO has no objection to government's proposal of engaging an independent data privacy expert to prepare the draft Code of Practice.	Will comply through the following measures : - to prepare the Code of Practice on ROP data in collaboration with the PCO; and - to engage a data privacy consultant to conduct the 4th PIA and to draw up the draft Code of Practice.

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		properly addressed in the document. In drawing up the COP, we understand that ImmD will work in collaboration with the Privacy Commissioner for Personal Data. We consider that the document should cover the aspects of collection, retention, use, security, access and disclosure of ROP data.		
4.	ROP forms should be revised to indicate more clearly the purpose of collection of personal information for the REO to address potential privacy concerns. (Disclosure and Policies)	Both the 1st and 2nd PIA recommended that the "statement of purpose" included in the ROP forms (e.g. ROP 1) be reviewed. Specifically, the 2nd PIA recommended a few amendments to be made to certain items of the "statement of purpose". In response to the 2nd PIA recommendations, ImmD had already addressed some of the privacy concerns over the "statement of purpose" (refer to Section 2 "Implementation Status of the 2nd PIA" item 13 of this report for details). At the time of the 3rd PIA, certain ROP forms have been revised and new ROP forms have been added as a result of the SMARTICS implementation. Amongst the changes to the ROP forms, we noted that certain wordings on the ID card application forms, ROP 1 (revised) and ROP S1 (new), are potentially unclear with respect to the fact that the provision of personal data to the Registration and Electoral Office ("REO") by the ID card applicant is voluntary. Both Part C of ROP 1 (revised) and Part D of ROP S1 (new) contain the heading: "To be completed by the applicant who is a registered elector". Under these Parts, a tick box is provided to the applicant with the following statement: "I am a registered elector. I understand that my personal data, as provided for in this application form, will be forwarded to the Registration and Electoral Office for the updating of the electoral register." The "statement of purpose" on the back of the forms states that "The provision of personal data to the Registration and Electoral Office is voluntary." We consider that without specifying clearly the voluntary aspect on the front of the form may bring about confusion	Wants to know which data items will be passed to the REO and whether it is possible to print the revised consent statement (i.e. consent to the transfer of personal data to REO) on the front page of the application form.	Will comply. The ROP forms will be revised upon its next reprint. Separately, ImmD has confirmed that only the English name, Chinese name and CCC code (if any), ID card number, ROA status indicator, DOB, sex, address and telephone number will be passed to the REO. ImmD will also add an asterisk to the revised consent statement to make it clear that it is an optional item.

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		and/or uncertainty to the applicant as to his/her right to choose whether to provide their personal data to another government department as part of the new Smart ID card application process. While we recognise that this is a good opportunity for the REO to update their records, for example, contact addresses and telephone numbers, it would be privacy positive to make the voluntary aspect of providing personal data to the REO more transparent to the applicant. We recommend that the ImmD to consider revising the statement on the front of the application form in future. The ImmD could consider using wording as follows: "I am a registered elector and I give permission for my personal data, as provided for in this application form, to be forwarded to the Registration and Electoral Office for the updating of the electoral register." Alternatively, the whole Part may be marked as an optional item by adding an asterisk "*". Clear communication is important to reduce privacy concerns that the public may have in relation to the new Smart ID card application process and the concerns over the provision of personal data to other government departments.		
5.	The Principal Immigration Officer (Information Systems) Production should be involved with all change requests to the SMARTICS post implementation. (Manual Procedures)	We note that the new Smart Identity Card System Control Section (established in May 2003) will be responsible for monitoring/approving any user change requests after the live-run of the system. This is in accordance with the long established change request procedures for other production systems. However, the primary role of the system controller is not to ensure that all privacy aspects of any system changes/enhancements have been considered. We understand that currently, the Principal Immigration Officer (Information Systems) Production ("PIO") is responsible for any privacy questions in relation to concerns and complaints raised by the public. However, the PIO has not been involved in the design and development of the SMARTICS and is not responsible for the privacy	--	Compliance achieved. PIO(IS)P is already involved in considering all post implementation enhancement requests as he is the Division Head of all the system control sections. In addition, another post has been created to oversee all privacy-related system changes/enhancement activities in ImmD.

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		compliance within the ImmD. His role is mainly co-ordination. Nevertheless, given the experience of the PIO's team in terms of privacy, there will be benefits if the PIO (or his team) is involved in the program change process from a privacy angle after the implementation of the SMARTICS. This will help to ensure that potential privacy concerns of the ID cardholders are taken into consideration and that future change requests are in compliance with data protection principles of the PD(P)O as well. Generally speaking, the involvement of the PIO/and his team, in the areas of privacy after system go-live in the program change control process could include: • To ensure privacy related issues are being undertaken before any system development. • To ensure the privacy aspect has been considered in the testing scenario. • To ensure user has tested the system thoroughly, particularly in areas relating to privacy areas, before signing off the test results. • To ensure changes in the relevant legislation have been reflected in the system design on a timely basis. It is also recommended that the PIO and his team sign-off on significant System Change Requests from a privacy viewpoint. We also note that the ImmD is considering to establish a new post called the Principal Immigration Officer (Records and Data Management) who will be responsible, among others, to actively manage and monitor on-going privacy compliance. If this position is approved, he/she could be responsible for the activities noted above. See additional details in Findings #6 Role of the proposed Principal Immigration Officer (Records and Data Management). Otherwise, the ImmD could consider expanding the role of the PIO to take on a more formalised role as a Chief Privacy Officer within the		

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		department who is responsible to formulate a privacy compliance strategy for the ImmD and to centralise/monitoring compliance throughout the ImmD.		
6.	The role of the proposed Principal Immigration Officer (Records and Data Management) could be further enhanced and expanded. (Disclosure and Policies)	We understand that the Information Systems Branch of the ImmD is planning to implement a new post, a Principal Immigration Officer (Records and Data Management) ("PIO") as part of their re-organisation. The position is, among other things, to oversee the ImmD's compliance with the provisions of the Personal Data (Privacy) Ordinance. The implementation of this new role is an important recognition of the need to manage new legislative and regulatory requirements (the future COP), and address increased scrutiny and concerns of Hong Kong residents. If this position is approved, the current job description of the PIO could be expanded to consolidate the various privacy related activities conducted throughout the organisation including:- • the development of the privacy strategy • assist with designing and implementing the new Code of Practice • conduct periodic privacy compliance reviews throughout the organisation • review initiatives with other departments / bureaux to assess the privacy implications • manage privacy awareness and training • address new privacy compliance concerns as they emerge • oversee enforcement-related activities such as the ImmD's response to subject access requests, complaints, and claims relating to data privacy	--	Compliance achieved. A dedicated post has been created to co-ordinate with Divisions concerned to oversee the proposed privacy-related activities. Advice will be sought from the 4th PIA consultant to develop appropriate monitoring mechanisms/tools and reports to assist him.

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		It is important that the PIO (also known as a Chief Privacy Officer in commercial organizations) has appropriate monitoring mechanisms/tools and reports to assist him/her with his/her duties. For example, the SMARTICS contains many audit logs, however, only a subset will be relevant to monitor privacy compliance, e.g. a report which identifies access grant to individuals of inappropriate rank. However, if this new post is not approved, the ImmD could consider whether the PIO(IS)P could take on the activities described above.		
7.	Procedures should be developed to ensure proper authorisation is required prior to enabling full Intrusion Detection System logging. (System Controls and Access Security)	The SMARTICS design includes the use of an Intrusion Detection System (IDS) that has the capability to perform full logging of data sent across the network segments being monitored. If full logging were to be enabled, large amounts of personal data would be captured in the IDS logs. We understand that the IDS is currently configured such that full logging is not enabled and that user accounts have not been granted access to these sensitive logs. However, we also recognise that at some point in the future it may be necessary to temporarily enable full logging to capture/ trace network security events or assist with solving network problems. The Smart Identity Card System Control Section will be responsible for approving any changes in accordance with the change request procedures. Since the full IDS logs may contain large amounts of personal data, these logs must be carefully controlled. We recommend developing measures that addresses the risk of exposure of personal data stored in the IDS logs. One way this could be achieved would be by requiring the Privacy Officer to: • Ensure that the logs are well controlled (i.e. unnecessary logs should be removed, adequate access controls should be placed on	Whilst appreciating that full logging of data is a necessary device to guard against the hacking of data, there is a risk that the IDS may be used as a "back door surveillance" tool if not properly controlled. To prevent abuse, the following measures should be implemented as a standing procedure: ◆ specifying the circumstances/criteria under which approval to full logging of data is allowed; ◆ the extent and amount of personal data to be logged under different circumstances; and ◆ the follow-up actions on the logs captured by the IDS,	Will comply. Procedures are being developed with recommendations from PCO included.

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		the logs, etc.), and • Approve any changes to the IDS configuration that would impact the amount of personal data captured in the logs.	which should be more stringent than other audit logs.	
8.	Ensure adequate controls and procedures are in place over message system that may contain personal data (e.g. MQ Dead Letter Queue). (System Controls and Access Security)	SMARTICS uses MQSeries middleware to send messages containing personal data between ImmD systems across the ImmD internal network. This personal data may end up stored in the MQ Dead Letter Queue. We recommend developing a housekeeping job to delete unnecessary messages in the dead letter queue on a regular basis. We understand that this is being implemented.	--	Compliance achieved.
9.	Privacy protection measures should be included in the outstanding sections of manual procedures that are being finalised. (Manual Procedures)	Key manual procedures to be followed in the SMARTICS production environment have already been developed, including the following areas: • Registration of ID cards • Processing of applications • Delivery of new ID cards • Issuance of ID cards • Disposal of old ID cards • Provision of records • Retention of records The ImmD has incorporated privacy protection measures into the above manual procedures to ensure compliance with the PD(P)O, ROP Ordinance and Regulations and other relevant Ordinances. However, procedures in relation to the new Smart Identity Card System Control section, operations under LAN/stand-alone mode, handling of uncollected Smart ID cards, usage of hand-held devices, and other ImmD sections outside the ROP Sub-division are being finalised at the time of the 3rd PIA. Privacy protection measures such as the following should also be considered in the development of	--	Will comply. Privacy protection measures will be incorporated into key manual procedures as appropriate.

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		these manual procedures: • Smart Identity Card System Control Section – this is a new section formed to provide system support to the SMARTICS in the production environment, such as user profile management and system security monitoring. We understand that the new Smart Identity Card System Control section will follow similar procedures as the existing system controllers, however, it is also important to ensure that there will be adequate privacy protection measures to be included in the specific procedures for this new section, such as the following: - Formal processes for addition, removal and change of regular and temporary user access rights. - Regular review of security related audit logs such as the authentication failure summary and the access reject summary as discussed in finding #1 of this report. - Periodic review of system security measures. - Due to the privileged access rights granted to the SMARTICS controllers, there should be monitoring procedures established to ensure tasks performed (e.g. maintenance of user profiles and user groups) by the staff of the Control Section are checked by their supervisors for proper authorisation and accuracy. • Operations under LAN/stand-alone mode – as a contingency measure, the ROP system is designed to operate in LAN/stand-alone mode when the connection to the main ROP database at ImmD Head Quarter is lost. Privacy protection measures should also be built-in to the manual procedures under contingency operations to ensure personal data is safeguarded equally as under normal operations. Specifically, there should be manual checking of an applicant's Limit of Stay ("LOS") to ensure that it has not been expired on the Smart ID card issuance		

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		date. After switching back to the normal mode, there should also be steps to ensure exceptions resulted from the recovery process are properly resolved. • Other ImmD sections outside the ROP Sub-division – the SMARTICS will be used by a number of sections, other than the ROP offices, within the ImmD (e.g. Immigration Control Point, etc.). Manual procedures in relation to the use of the SMARTICS should be developed for relevant sections of the ImmD to ensure that there are adequate privacy measures on handling of personal data. For example, each of these sections should have procedures to govern the proper use of the SMARTICS enquiry function on personal data. ImmD should ensure that manual procedures for the above areas be completed as soon as possible, and appropriate privacy protection measures similar to those recommended above included in the procedures.		
10.	The "Retention Period of files/records in ROP Sub-division containing ROP data" ('RPOR') document should be updated. (Manual Procedures)	The 'Retention Period of files/records in ROP Sub-division containing ROP data' document is a document that specifies the defined retention period of different types of physical documents or records containing ROP data. At the end of the retention period, the related documents or records will be destroyed accordingly. The launch of the new ID card has resulted in a number of newly created/modified physical documents or records, however, we noted that the RPOR document has yet to be updated to reflect all the new changes. Without specifying clearly the retention period of different types of physical documents or records, there may be confusion and inconsistent treatment by users as to the appropriate period of retaining these documents or records that contain personal data. To ensure that personal data within these documents or records are not kept for a period longer than necessary in compliance with PD(P)O,	--	Will comply. Retention periods on different types of documents or records arising from the implementation of SMARTICS are being updated in the PROR. The document will be issued for staff to follow after finalization.

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		we recommend that the RPOR document be updated and improved wherever necessary to specify clearly the retention period of the complete set of new or existing physical documents or records produced from the new SMARTICS.		
11.	Reduce the risk associated with the use of hardware based keystroke loggers. (System Controls and Access Security)	We understand that simple usernames / passwords are used for authentication for all ROP system users, including privileged users such as system controllers. We also understand that software based controls have been implemented to prevent users from installing unauthorised programs (such as keystroke loggers) on workstations. These controls are designed to prevent or detect the installation of software based Trojan programs. However, these Operating System based controls cannot prevent the installation of hardware based keystroke loggers that have the capability to capture user names and passwords directly from the keyboard. Hardware based keystroke loggers that bypass operating system level controls and log keystrokes directly from the keyboard are now readily available in the market. These devices may be relatively simple to install and difficult to detect. Use of these devices may compromise the passwords of anyone who types his/her username and password into the workstation. We recommend to reduce the risk that hardware based keystroke loggers may be used to disclose the system controller's password by: a) Ensuring that the rooms in which the system controller's workstations are located are physically secured such that it would be difficult for any unauthorised party to access the system controller's workstations and install a keystroke logger; b) Developing guidelines or procedures that will require system controllers to normally login only to their own workstations; and	Apart from the three recommended measures, both "alternative (optional)" approaches suggested by the consultant, in particular the use of laptop computers which would not induce significant system changes, are effective means to reduce the risk of keystroke logging and should therefore also be considered.	Will comply through the following measures: - to ensure the rooms installed with system controllers' workstations are secure to prevent unauthorized party to access the workstations and install a keystroke logger; - to develop guidelines and procedures for system controllers to login only to their own workstations for carrying out their duties; - to develop guidelines and procedures for system controllers to visually inspect the keyboard cable connector prior to logging into any workstations other than the designated ones; and - to explore the use of laptop computers.

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		c) Developing guidelines or procedures that requires system controllers to visually inspect the keyboard cable connector prior to logging into any workstations other than their own. They should verify that an unauthorised keystroke-logging device has not been installed. Note that alternative (optional) approaches to reduce the risk for ImmD consideration include: a) Requiring the use of two-factor authentication to prevent the re-use of captured passwords, b) Preventing the installation of a keystroke capture device by physically securing the keyboard cable connection or using a laptop computer (which has no keyboard cable) that has been logically and physically secured.		
12.	Ensure that large amounts of personal information are not stored on workstation hard drives. (System Controls and Access Security)	We understand that most of the workstations do not use disk level encryption such as Windows 2000 Encrypting File System (EFS). As such, it may be possible to remove the hard drive from ImmD systems and view the data on them (such as Internet Explorer temporary files). When implementing the SMARTICS, we understand that large amounts of personal information cannot be found within temporary data files (such as cached web pages) stored on the hard drive. One approach to ensuring the implementation and detecting potential personal data on user workstations includes: a) Do a 'fresh install' of a user workstation PC, and securely configure it such that it matches the configuration that will be used in production. b) Use an integrity checking utility to record all the files (including temporary files) on the hard drive. c) Use the workstation to access a range of personal data and perform different types of transactions.	--	Compliance achieved.

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		d) After a period of time, use the integrity checking tool to detect changes to files (additions or modifications) on the hard drive. e) Examine changed files to determine if any of these files contain personal data.		
13.	A login banner should be displayed for the SMARTICS. (System Controls and Access Security)	The workstations accessing the SMARTICS do not currently contain a login banner that indicates that "unauthorised use is prohibited" and that "violators may be prosecuted". A login banner increases the awareness of users (authorised and unauthorised) of the implications and consequences of unauthorised access to the system. Access could be gained by a number of parties (e.g. internal users, contractors, consultants, etc.), through a number of means (e.g. at the terminal, remotely, etc.). We understand that there are already some controls in place to assist with prosecution of unauthorised access by ImmD employees (i.e. security undertaking users must agree to as part of their employment). If external parties were to gain unauthorised access to ImmD resources, they could argue that they were unaware of the violations. We therefore recommend to install a login banner that indicates unauthorised access is prohibited and violators will be prosecuted.	--	Compliance achieved.
14.	Initial password for newly created user accounts in the SMARTICS should be unique. (System Controls and Access Security)	We note that the default password for all newly created user accounts is the same in the SMARTICS. By implementing a standard initial password for all new user accounts increases the risk that new user accounts could be tampered with or used by unauthorised individuals before the designated personnel has a chance to change their initial passwords at first log-in. For example, an ImmD staff can easily guess the user id of a colleague or new member simply by using the initial and surname of the staff and then log into the system with the standard initial password. If the new user account is granted with	--	Compliance achieved.

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		access to personal data, then the unauthorised user will also have access to the personal data. ImmD should consider assigning a random initial password to each new user and this password should be difficult to guess. Delivery of the initial password to the end user should be in a confidential manner, which means only the intended recipient of the user id should know the initial password.		
15.	Personal data enquiry functions should be granted on a need-to-have basis (System Controls and Access Security)	The SMARTICS has five main enquiry functions that allow users to search for personal data stored within the system. Depending on the enquiry function being used, users can view on-screen and/or print the personal data of ID card holders that met the search criteria. From a privacy standpoint, it is important to ensure that only those users who genuinely require one or more of these enquiry functions should have such access rights. We recognise the system has an audit log function that allows designated ImmD officers to review the enquiries being performed by users in the system (refer to finding for recommendation on the review of this type of audit logs). At the time of the 3rd PIA, the matrix which defines access rights for different job roles has yet to be finalised and approved by user management. However, we noted from this matrix the following exceptions with respect to the SMARTICS enquiry functions and that the ImmD should consider whether they are actually needed: • Clerical Officer ("CO") under Personalisation Office of ROP Records Section has been granted with "ROP Full Data Enquiry" and "ROP Key Data Enquiry (ROP Enquiry)" • Clerical Assistant ("CA") under Records Maintenance Office of ROP Records Section has been granted with "ROP Key Data Enquiry (ROP Enquiry)" We understand that the job descriptions and manual procedures in relation to the CO and CA roles above do not require performing	--	Compliance achieved. At the time of the 3rd PIA, the matrix defining access rights for different job roles, was only a draft. During the 3rd PIA, the matrix was finalized without granting the CO/CA in question the access right to the ROP data enquiry.

Item	Issues	3rd PIA Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data	Government's Response/ Way Forward
		enquiry on personal data within the ROP system. To ensure personal data is only accessible by authorised users on a need-to-have basis, the enquiry functions proposed for the above CO and CA roles should be reassessed.		