Information paper on
6 February 2001

Panel on Security of the Legislative Council

**HKSAR Identity Card Project —
Initial Privacy Impact Assessment Report**

On 16 January 2001, Members were given a copy of the initial Privacy Impact Assessment (PIA) Report. We undertook to share with Members the Administration's views on the various proposals in the Report.

2. We have discussed the findings of the initial PIA report with the Office of the Privacy Commissioner for Personal Data (PCO). Overall speaking, we agree with the consultants and the PCO that, most important of all, we have to work out a comprehensive data privacy strategy encompassing the following areas -

(a) Legislative aspect – to ensure that the necessary data privacy safeguards are laid down in law so as to deter abuses and to gain the confidence of the public;

(b) Administrative aspect – to ensure that the necessary procedural safeguards and code of practice are drawn up;

(c) Technical aspect – to ensure that the necessary security and privacy enhancing technologies are built into the system;

(d) Publicity aspect – to ensure that the general public fully understand what they can do with their ID cards, the choice where relevant they have with the applications on offer, and their data privacy rights.

3. In sum and in general, we find the proposals in the PIA Report acceptable. For ease of reference, the data privacy issues/proposals identified by the consultants, the PCO's comments and the Administration's response are summarised in the table at Annex.

Security Bureau
2 February 2001

Annex

Initial Privacy Impact Assessment
Summary of Recommendations

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
PART V – PRIVACY IMPACTS ANALYSIS			
Legislative Framework			
63 (Legislation)	The statutory framework for the Registration of Persons (ROP)/ID Card system should be reviewed to ensure that it provides a comprehensive basis for the HKSAR ID Card system as a whole.	-	Will review.
Multiple Applications			
64 (Principle)	If any additional applications or uses are considered for the HKSAR ID Card, they should ideally be voluntary at the entire discretion of the card holder instead of making the choice of application merely on practical necessity.	The citizens should be free to choose the applications on offer. Subscription to the applications should be voluntary.	Possibly with the only exception of the driving licence, card holders will be free to choose whether to include additional applications in the smart ID card. There is community acceptance to this approach, based on the outcome of the public consultation so far. Will discuss further with PCO and consult the views of the relevant LegCo Panels when the feasibility studies of other applications are completed.
Card Management			
65 (Principle)	Privacy concerns would be lessened if ImmD retained in-house all aspects of the card scheme management and the possibility of the function being performed by any other government agency, or being outsourced, was expressly ruled out.	The ImmD already asserts that it will keep control over all aspects of registration and card-issue.	ImmD will definitely undertake the card registration and card issue functions. The Administration will ensure that all aspects of the card scheme management, including the management of other value-added applications, are secure and will protect the privacy of individuals.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
78 (Principle)	If the card is to hold other applications, there raises privacy concerns about :- ■ the smart card scheme operator being a separate government agency; ■ 'outsourcing' of card management; ■ the smart card scheme operator was a commercial operator, either through 'outsourcing' or as a joint venture; and ■ limited range of administrative aspects being handled by another agency and the ImmD would keep control over all aspects of registration and card-issue.	It is appropriate to have a high level inter-departmental working group to assess the type of non-ID card applications to be included. ImmD must be a member of this inter-departmental working group such that it is aware of the potential applications, and to ensure that none of these applications would in anyway infringe upon the security, integrity and use of the personal data within the ImmD's domain.	For the card management :- ■ outsourcing the management work to a commercial operator has been ruled out; ■ on ID card matters, ImmD will remain responsible for the registration and issue of ID cards and the maintenance of the application records; ■ on non-ID card matters, a high level inter-departmental Steering Committee chaired by SITB has been formed to take care of the multiple application aspect of the smart card scheme. The Steering Committee will make recommendations on the types of applications to be included in the new ID card. ImmD is a member of the Steering Committee. The "scheme operator" is a team of technical people to provide technical advice and support service on the multiple application aspect of the smart ID card scheme, e.g. provide help desk service, certifying equipment, etc. They will have no access to the data which are kept by individual departments. We are conducting various feasibility studies with regard to the implementation of multi-applications. Based on the findings of these studies, we will firm up the design on all aspects of the card management scheme giving due regard to privacy concerns. In any case, we have no intention to outsource the card management.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
Implications of Cryptographic Functions			
67 (Technical advice)	If the cards are to be capable of supporting cryptographic functions, the private keys, for both digital signature and message-encryption purposes, should be generated on the chip alone to ensure maximum privacy protection.	-	Will be considered in the feasibility study on digital certificate.
The Functions of the ROP Sub-System and Manual Procedures			

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
71/72 (Procedure) 87/88 (Technical advice)	It appears that the omission of the thumbprint from the ROP database would have a limited negative impact (some relatively minor inconvenience for those who have lost or damaged cards), in return for a very considerable reduction in the system's privacy-invasiveness. An alternative approach would be for the ROP database to carry only the thumbprint template. ImmD should: ■ design alternative processes and procedures to handle a situation in which thumbprints are not held on the ROP database, or are held only in template form; ■ in the Request For Tender, require tenderers to provide proposals relating to alternative implementations in which the ROP database contains the thumbprint, contains only a template of the thumbprint, and contains neither; ■ conduct trials to confirm that these procedures do not significantly reduce the integrity of the scheme, nor unduly increase the efforts and costs of individuals or the ROP Registration Office; subject to satisfactory outcomes of these trials, implement the system without storing the thumbprint in the ROP database.	While the storage of digitized thumbprint on the ROP database would arguably provide the least hassled procedure to re-establish the identity of holders of lost or damaged cards, the corollary is the virtual creation of a population database with a unique biometric identifier which can be matched with ease for every person. The non-storage of the thumbprint in the database, or just the storage of the template, should be further explored in the forthcoming tender which could lead to other creative and effective alternatives to process stolen or lost cards. If it is a preferred solution to store thumbprint data on the ROP database, the feature should be accompanied by legislative / regulatory protection prohibiting access to such data for non-immigration purposes and prohibiting the one-to-many matching searches as well as stringent access control on the database.	Have serious reservation to omit the thumbprint from the ROP database. Without the thumbprint which is the record of last resort and the unique key for verification of identity, ImmD shall not be able to quickly and positively authenticate if a person is the rightful holder of a lost or damaged card. More importantly, the proposal would adversely affect the speed in re-establishing the identity of distressed Hong Kong residents who have lost their identification documents and are stranded in overseas countries. In normal circumstances, most foreign governments will only provide the thumbprint impressions to ImmD for verification. While the quality of the thumbprint impressions are normally adequate for visual checks against the thumbprint records kept by ImmD, they may not be good enough for the generation of templates for matching purpose. Delays will occur if we need to ask the government concerned to take another set of thumbprint impressions. The storage of raw and encrypted fingerprint images in the ROP database is preferred to the storage of templates because the latter will make one-to-many matching much easier. The use of proprietary biometrics template techniques will also lead to vendor lock-in. We should avoid this risk because it is impractical to ask the whole population to provide the thumbprints again if the vendor runs out of business. In view of PCO's advice, we will explore in forthcoming tender whether vendors could provide creative suggestions which would address the concerns of both sides. We also agree that if a decision is taken to maintain the thumbprint images in the ROP databases, we will work out the appropriate legislation/regulatory and technical measures (e.g. encryption of thumbprints) to restrict access to such data and to re-assure the public that there will not be one-to-many matching searches, as we have committed publicly before.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
Collection			
82 (Procedure)	ImmD will need to ensure that the statement of purpose and of the parties to whom the personal data may be transferred [Data Protection Principle (DPP)1(3)(b)(I)(B)] keeps pace with the actual uses and disclosures of personal data, both now and particularly under the new system.	-	Will comply.
82 (Procedure)	ImmD should review the adequacy and accuracy of its 'statement of purpose' included on forms to satisfy the underlying objective of DPP 1(3).	-	Will comply.
83 (Procedure)	ImmD may wish to consider whether arrangements can be made for a range of individuals who have special circumstances or needs. These include, potentially: ■ persons-at-risk (various categories described under Special Arrangements on p.79) ■ public figures, whose participation in normal registration processes might cause difficulties either for them or for ROP staff; and ■ persons with genuine objections to the standard processes for capturing photograph or thumbprints, either for religious or conscientious reasons or because of disfigurement.	-	Some of the suggested special arrangements e.g. non-capture of thumbprint, additional ID cards, etc, will adversely affect the integrity of the ROP database. For the sake of fairness, we will have to treat all residents alike. But if there are good reasons, we will consider providing special assistance on a case-by-case basis.

Note : Data Protection Principle (DPP) means the principles set out in Schedule 1 of the Personal Data (Privacy) Ordinance

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
Data Quality			
83 (Legislation)	ImmD needs to review the need for the items of information required under ROP Regulation 4 to be updated.	-	Will review.
84 (Legislation)	Consideration should also be given to statutory amendments to give legal protection to individuals against 'presumption of guilt' due solely to technology failures (e.g. corrupt or damaged cards, card-receiver failure, loss of communications links).	-	Hong Kong law is based on 'presumption of innocent'. According to legal advice, legislative amendment will not be required for this purpose.
84 (Procedure)	ImmD should review its records retention policy and develop and implement a disposals schedule in respect of all personal data, in all storage media, to comply with the requirements of DPP 2(2) and s.26 of the Personal Data (Privacy) Ordinance (PDPO) in relation to retention and erasure of data when the purpose for holding it has expired.	-	At present, ROP records are kept for a long period of time even if the person concerned was deceased because the data will still be needed for a variety of purposes, in assessing claims to right of abode or applications for Certificate of Registered Particulars by descendents. We will, however, review the record retention policy to ensure that the requirements of DPP 2(2) and s.26 will be complied.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
Use and Disclosure			
84 (Legislation)	Statutory amendments will be required to the ROP Ordinance and Regulations, and possibly to other laws, to provide for the new scheme, including specifically for the following elements: ■ reading of 'non-visible' card data by agencies other than ImmD; ■ provision of thumbprints in various scenarios for comparison with the prints recorded in digital form on the card.	The amendments to the ROP Ordinance with respect to data privacy protection should specify clearly ■ how the card scheme is to be administered and operated; ■ how the data on the card, the ROP database and associated images will be used; and ■ circumstances where ROP records are to be linked. ■ The amendment to ROP Ordinance should specify clearly the provision of criminal sanctions against any person attempting to store data, or to use/disclose data or to perform functions, on the card in a manner unknown to the person, against the person's wishes, and /or harmful to the person's interests.	Will consult PCO on the legislative amendments.
85 (Legislation)	ROP Regulation 24 should be amended to expressly cover all personal data held by ImmD in connection with the ROP function.		Will comply.
85 (Legislation)	Consideration should be given to moving the prohibition into the ROP Ordinance itself, or any amendments made subject to the express approval of LegCo (i.e. positive disallowance), so that it cannot be overridden by pre-existing provisions in Ordinances giving a power to obtain information.		Will comply.
85 (Legislation)	Any subsequent legislative provisions to authorize disclosures of ROP information should also be subject to a positive approval process in LegCo.		Will comply.
85 (Legislation)	The ROP Ordinance should make *all* unauthorized use (including 'mere' browsing), and including unauthorized disclosure of the information concerned, an offence, subject to suitable penalties.		Will need to look at the issue further with Department of Justice as to the establishment of mens rea, in cases of 'mere' browsing.
85 (Procedure)	ImmD should ensure that all disclosures from the ROP database and other records (whether provided directly or via an ability to read card data) are authorized by relevant permission under ROP Regulation 24.	-	This is already the case. Will continue to comply.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
85 (Procedure)	With regard to matching procedures, ImmD will need to ensure that any requests for further automated matching under the new system meets the definition of matching procedure in the Personal Data (Privacy) Ordinance and endorsed by the Privacy Commissioner.	-	This is already the case. Will continue to comply.
85 (Principle)	Privacy concerns about the use of personal data held on, or supplied in connection with, the HKSAR ID Card would be significantly reduced if ImmD, or the government as a whole, were able to give commitments: ■ that the card will not be contactless; ■ that the details which are permitted to be displayed on the card will be no more than those envisaged in the Feasibility Study Report; ■ about the specific data items that may be stored in the chip; ■ about the organizations or classes of organizations permitted to access data directly from the chip, and for what purposes; ■ about the organizations or classes of organizations permitted to take (or read) thumbprints for the purpose of comparison with the digitized print on the card, and the circumstances in which this will be permitted; and ■ about the circumstances under which conversion of any of the information which is merely imaged (previously microfilmed) into fully machine-readable form is permitted.	-	Agree in principle. ImmD will probably use contact smart cards but have reservation to expressly rule out the use of contactless cards. This is because with the change in technology, it is quite possible that contactless cards can be as secure as contact cards.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
86 (Principle)	Person-to-person linkage is a very privacy-invasive activity. ImmD should ensure that provision of 'associated person' data (e.g. parent-child, guardian-child & spouses etc.) to authorized agencies is covered by proper legal authority. That is, permissions issued pursuant to ROP Regulation 24 are worded so as to allow 'associated person' data to be disclosed.	-	Agree in principle.
Security			
86 (Principle)	The data stored on the card chip for the ROP/ID card application should be subject to all of the limitations embodied in the Feasibility Study (FS) Report, in particular that they are :- ■ limited to the data-items currently envisaged and set out in that Report; ■ subject to the specified technical protections; and ■ accessible only by the specified and very limited number of devices and organizations for the specific purposes stated.	Adequate security features including appropriate hardware, software, encryption of data and administrative measures are required to prevent unauthorized or accidental access to and disclosure of data in the card and personal data in the related application databases, to preserve data confidentiality, integrity and accuracy.	Will comply with PCO's comments.
86 (Technical advice)	The system specification for the new system should expressly include the segregation of data, functions and applications as well as limited conveyance of information by card number that it currently does.	-	Agree in principle, but subject to the views of the consultants who are studying the multiple application side of the system.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
87 (Technical advice)	The Request For Tenders (RFT) should explicitly require proposals to explain precisely how integrity of data and functions will be protected with details of hardware, system software and application level features. The card should perform challenge to and authentication of devices and processes with which it interacts, and only participate in processes where the results are satisfactory, in order to provide protection of the data against disclosure to, and of processes from performance by, unauthorised parties. The card should participate effectively in the authentication of the person presenting it so as to prevent the exercising of the cardholder's prerogatives by an imposter.	Supports Consultant's recommendations with emphasis.	Will comply.
87 (Technical advice)	It is highly desirable that the biometrics stored on the card do not leave the card under any circumstances. The RFT should invite tenderers to address this issue. It should be made a 'highly desirable' feature that would weigh significantly in the assessment of tenders, if it proves to be available.	The biometrics should not leave the card or be copied. The comparison of the thumbprint template should be done by processor on the card as biometrics data being stored in the card receiving devices would pose necessary risks of interception.	Agree in principle but subject to technical study, in particular, the transaction response time. Will invite tenderers to look into the issue and propose solutions.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
87 (Technical advice)	If the cards are to be capable of supporting cryptographic functions, then the following additional specifications should be included: ■ the card must perform secure key-generation, and provide secure key-storage and secure key usage for both digital signature and message-encryption key-pairs; ■ cardholders must be given the choice concerning the number and usage of key-pairs and certificates acquired; ■ any backup arrangements for private keys need to be entirely at the discretion of the cardholder, such that individuals have a genuine choice of organizations offering back up services, including non-government service providers; ■ no government agency should be able to gain access to any such backup; and ■ compulsory escrow arrangements for private keys must be precluded.	-	The future FS on digital certificate will take into account those recommendations on key generation and storage. Will consider the suggested backup arrangements for private keys.
87 (Principle)	Privacy concerns would be eased if ImmD could confirm that the digital thumbprint will only be used for one-to-one comparisons for the purpose of authenticating the claim of identity of a person, and for no other purpose, especially for one-to-many comparisons in order to identify a person from their thumbprints.	-	Will comply.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
88/89 (Technical advice)	An appropriately qualified independent technical consultant, should certify, following a technical audit, that the design and implementation of the scheme ensures that the following risks have been comprehensively and effectively addressed:- ■ the risks of using the card to store and disclose data unknown to the person and to perform functions unknown to the person; ■ if the key is to support cryptographic functions, the risk that a private key could be discovered and invoked by a person other than the cardholder; ■ in relation to card-reading devices, the risk of :- - interception of traffic, and hence access to personal data or access to a stream of data; - the recorded biometrics becoming capturable by other agencies, organizations or individuals; - other organizations seeking to capture the biometrics themselves, as a more efficient means of authentication than visual inspection of the ID Card; - the recorded biometrics being obtained illicitly and used by imposters to masquerade as an individual; - the PIN or PINs being captured; - masquerade use of unsupervised devices by imposters who acquire the card and any necessary knowledge; and - card-data being amended by inappropriate devices.	Many aspects of the card-receiving devices are not known at this stage. PCO takes note that their privacy implications are to be tackled at subsequent PIAs and security audits.	Will look into these areas in the next PIA and the Security Audit.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
89 (Technical advice)	The new scheme should embody all of the privacy-positive security features that are in the existing scheme, including access controls and interface controls relating to other ImmD systems, and external systems such as ECACCS. Controls should apply at all times, including, for example, to mobile registration operations.	-	Will comply.
89 (Technical advice)	ImmD should work towards integrating access controls to its computer systems with its human resource management system(s), in relation to the timely invalidation of user ID/password pairs on departure of staff and during extended periods of absence.	-	Agree to work towards this direction although the proposal involves the integration of another system that is not yet well developed/computerized.
89 (Technical advice)	The specifications of the scheme relating to the gathering of logs and audit trails should be enhanced to ensure that sufficient detail is gathered.	-	Will comply.
89 (Technical advice)	The specifications for the scheme should be amended to require much higher standards of reliability and resilience than the "at least that of the current system" suggested in the Feasibility Study Report. Disaster recovery planning should be based on much more than the suggested "basic survival" mode.	-	Agree but subject to technical feasibility and cost effectiveness.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
89 (Principle)	ImmD should include understanding of the privacy issues associated with ID cards and their use, and the way in which these issues have been addressed, in training programs for relevant staff.	-	Will comply.
89 (Legislation)	Making it an offence to solicit (with or without payment) unauthorized disclosure of ROP data.	-	Will comply.
90 (Legislation)	Placing limits and/or conditions on the use of ROP data by persons or organizations to whom ROP data is disclosed (both directly pursuant to ROP Regulation 24 and indirectly under Regulation 23), and making it an offence to breach those limits/conditions.	-	Will comply.
90 (Principle)	ImmD should re-affirm its commitment to take disciplinary action against any officers or employees breaching security, and/or using personal data outside relevant legal authorities.	-	Will comply.
Openness & Transparency			
90 (Public Consultation)	Publication of aggregate statistics about disclosures of ROP information to other agencies would be a significant demonstration of commitment to this principle.	-	Will consider.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
90/91 (Principle)	It is partly in the spirit of the openness and transparency principle that Privacy Impact Assessments should be carried out in public, and with the widest possible input. While there has been no public input into this PIA to date, public release of the PIA report as soon as possible would be consistent with the objective of DPP 5 of the PDPO. Ideally, this PIA should be made public, to assist consideration of the proposal by legislators and other stakeholders. In addition to public release of the PIA, it should be given to key representatives of the public.	Findings of PIA studies and governments' responses to such studies should be publicly available.	An abridged version of the first PIA report has been distributed to LegCo Members. We will also disclose the results of future PIAs.
90 (Public Consultation)	Wider consultation about the HKSAR ID Card scheme would both engender confidence in the scheme, and enable ImmD to take account of any concerns in the design.	Different mechanism should be considered by the Government to further assure the trust and confidence of the community to subscribe to the applications on-offer.	The first round of public consultation was completed in December 2000. We will consult the views of the relevant LegCo Panel before other non-immigration applications are to be included in the smart ID card.
91 (Public Consultation)	In order to facilitate understanding amongst stakeholders, ImmD should make available technical briefing materials.	-	An abridged version of the management summary of the Feasibility Study Report on the new identity card system was issued to LegCo Members in early December 2000.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
91 (Public Consultation)	Given the tight timetable, ImmD could consider convening a public interest reference group, comprising key representatives, to provide an efficient channel for information about the proposal, and for feedback. Consultation would not therefore need to be completed in the immediate future and could proceed in parallel with the tendering process.	-	A special LegCo Security Panel meeting which was opened to the public and focus groups, was held on 11.11.2000. Besides, open forums to the general public and focus group were arranged on 6.12.2000 and 6.1.2001.
92 (Public Consultation)	There will presumably be a major public information and education campaign prior to the commencement of re-registration; and there will also need to be awareness and training activity associated with the proposed 'kiosks' at which individuals will be able to check the contents of their cards. Explanation of privacy issues and the ways in which they have been addressed should form part of these campaigns.	The citizens should know their inherent rights when using the card, what information the card contains and how it will be used. The citizens should be aware of, for each application, what personal data the card contains and who has access to it.	Being arranged.
92 (Public Consultation)	ImmD should incorporate material on privacy issues into public information campaigns and related activity preceding and accompanying the introduction of the new ID Card.	Raising public awareness on how privacy issues have been addressed in re-registrations campaign as well as in the launch of the various applications to come on-stream.	Done. Promotion leaflets contain concrete measures to be taken to address privacy concerns.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
Access & Correction			
92 (Procedure)	ImmD's approach to satisfying requests for access is to use existing statutory processes where they already exist. Most of the template certificates used in reply to such applications are designed to meet the particular needs. ImmD needs to ensure that responses to these requests satisfy DPP 6 and s.19 (1) of PDPO by providing all of the applicable personal data, together with whatever explanation may be required (e.g. of codes).	The citizens should be provided with the means to access, print and interpret the data on their cards and their personal data in the application databases, and if relevant, request for correction.	Already complied with.
92 (Procedure)	ImmD should review its processes for responding to subject access requests under DPP 6 to ensure that individuals are given access to all the ROP data to which they are entitled.		Already complied with.
Privacy Impact Assessments			
93 (Expert advice)	The RFT should be formally reviewed, prior to despatch to vendors, by persons with specialist expertise in the privacy aspects of schemes of this nature, to ensure that any additional privacy-positive measures adopted as a result of this PIA Report have been translated effectively into tender specifications.	-	Will incorporate into RFT privacy features and additional privacy-positive measures as recommended in all PIAs and agreed by the Administration. Will consult PCO before finalizing the RFT.
93 (Expert advice)	The selected tender should be reviewed, prior to finalisation of the contract, by persons with specialist expertise in the privacy aspects of schemes of this nature, for its conformity with the privacy requirements of the RFT.	-	Will vet tenders carefully to ensure conformity with the privacy requirements of the RFT and consult PCO before finalisation of contract.

Page No. (Nature)	Consultant's Views / Recommendations	Comments from the Office of the Privacy Commissioner for Personal Data (PCO)	Government's Response/ Way Forward
Overall Privacy Strategy			
95 (General)	ImmD needs to recognize the very substantial privacy implications of the proposed scheme, and the resultant need for an integrated strategy in relation to all of the following: ■ legal authorizations and constraints; ■ consultation, preferably directly with the public, but at least with key representatives; ■ technical specifications; ■ organizational policy commitments; ■ compliance with the Personal Data (Privacy) Ordinance; and ■ public awareness, education and training campaigns. Implementation of an integrated privacy strategy will involve a combination of legislative amendments, policy commitments, and specifications in the scheme design, tendering, contractual and implementation stages of the project.	Supports and echoes the Consultant's recommendations	We have discussed the matter with PCO and agreed that our privacy strategy should encompass the following areas :- (a) Legislative aspect – to ensure that the necessary data privacy safeguards are laid down in law so as to deter abuses and to gain the confidence of the public; (b) Administrative aspect – to ensure that the necessary procedural safeguards and code of practice are drawn up; (c) Technical aspect – to ensure that the necessary privacy enhancing technologies are built into the system; (d) Publicity aspect – to ensure that the general public fully understand what they can do with their ID cards and their data privacy rights. We will conduct further PIAs at different stages of the project. We will also develop a code of practice jointly with the PCO.