[LCQ15: Implementation of electronic identity system]

Following is a question by the Hon Charles Mok and a written reply by the Secretary for Innovation and Technology, Mr Nicholas W Yang, in the Legislative Council today (April 17):

Question:

The Government will launch the electronic identity (eID) system in 2020. Gradually, as many as 100 public services will make use of the biometric authentication technologies (including facial recognition, fingerprint identification, iris recognition and voiceprint recognition) of the eID system to authenticate the identity of service users. On the other hand, the Government awarded service contracts for the implementation of as well as support and maintenance for the eID system to three contractors in February this year. The offices of two of the contractors are located in Shenzhen. In this connection, will the Government inform this Council:

(1) of the respective weightings for the price and technical aspects in the score for the tendering exercise for the eID system; as the system involves the handling of a huge quantity of personal data of members of the public, whether the Government attached more importance to the bidders' information security technology capabilities and track records when determining their technical scores;

(2) of the following information on the service contracts for the eID system:
(i) the specific division of duties among the three contractors, and the timetable for the various items of work during the contract period which lasts for eight and a half years,
(ii) whether it has been stipulated that all development, testing and maintenance work must be carried out within the territory of Hong Kong; if not, whether it knows the place(s) where the relevant work will be carried out, and
(iii) whether it has required the contractors to engage, at various stages of the system, independent consultants to conduct information security audits on the programme codes of the system to ensure that the system does not contain any backdoors or security loopholes;

(3) whether it knows if the three contractors will subcontract the relevant work; if they will, (i) whether the subcontractors are companies registered in Hong Kong and what track records in related businesses they have, and (ii) the measures in place to ensure that the personal data of members of the public will not be transmitted to places outside Hong Kong;

(4) of the following information on the facial recognition data, other biometric authentication data and other personal data handled or collected by the eID system respectively (a) during the development and (b) after the

coming into service of the system:
(i) the respective locations of the servers at which the various sets of data are stored (i.e. government data centres, offices of the contractors or other premises, and whether those places are situated within the territory of Hong Kong),
(ii) the data encryption standards to be adopted,
(iii) the information security precautions in place to prevent data from being intercepted or altered in the course of transmission,
(iv) the authority of and restrictions on the access to personal data by government officers and staff of the contractors, and
(v) the security mechanism for preventing unauthorised access to personal data (including prescribing the authority of and restrictions on the access to personal data by the development and maintenance staff);

(5) whether the various sets of data mentioned in (4) will be used for other purposes; if so,
(i) of the government departments or public organisations which will use the data and what such uses are,
(ii) of the personnel who will have the authority to access the relevant data,
(iii) of the means of obtaining the data (such as being permitted to login the eID system or provided with a copy of the data), and
(iv) of the measures in place to ensure that government departments or public organisations will take sufficient information security precautions to prevent data from being intercepted or altered in the course of transmission; and

(6) whether, in developing the eID system, the Office of the Government Chief Information Officer has (i) consulted the Privacy Commissioner for Personal Data, and (ii) engaged an independent third party to assess the information security risks and privacy implications; if so, of the details, and whether the relevant view(s) and assessment report(s) will be made public?

Reply:

President,

Our reply to the six parts of the question is as follows:

(1) Information security as well as the protection of personal data and privacy were essential requirements under the tender documents for the electronic identity (eID) system, which included security requirements in data storage, network communication, user management and application systems and the security measures to safeguard personal data in accordance with the provisions of the Personal Data (Privacy) Ordinance. In addition, to align with the pro-innovation government procurement policy, a weighting of 60 per cent for technical assessment was adopted in the marking scheme of the tender for the eID system, of which about seven per cent was related to information security.

(2) The contractors of the eID system are required to complete system

development in the first 18 months of the contract period, followed by a 7-year system maintenance period. The division of work among the three contractors are as follows:

(i) Ping An Technology (Shenzhen) Co., Ltd. is responsible for the design, implementation and support of the eID core system, as well as the facial recognition and image processing system;

(ii) ICO Ltd. is responsible for the design, implementation and support of the system which verifies the identity of eID users by using the data of the Immigration Department; and

(iii) Shenzhen Emperor Technology Co., Ltd. is responsible for the design, manufacture, supply, management and support of the self-service registration kiosks and the registration tablets.

As specified in the tender documents, the contractors are required to arrange key staff (project managers, systems architects, systems analysts, cloud computing specialists, etc.) to work in the office premises designated by the Office of the Government Chief Information Officer (OGCIO). This is in line with the general work arrangement for major projects to facilitate close communication between the OGCIO staff and the contractors, problems being resolved in a timely manner and monitoring the work of the contractors such as confirmation of the detailed system design, and progress of system development, integration and testing. The tender documents do not strictly require all system development work to be carried out in Hong Kong. We understand that the contractor mentioned in (2)(i) above will carry out programming related tasks in its facilities in Shenzhen. The OGCIO will examine in details the programmes submitted by all contractors to ensure compliance with the contract requirements and the government information technology (IT) security policy and guidelines before performing system integration and testing.

The OGCIO will engage independent third parties at different stages of the implementation like system design, system development and testing, system operation, etc. to conduct privacy impact assessments, privacy compliance audits and information security risk assessments and audits, which include source code review and penetration tests, to protect personal privacy and ensure system security.

(3) As specified in the tender documents, the contractors were required to name the sub-contractor(s) in their proposals if there would be sub-contracting. The contractor mentioned in (2)(i) above indicated in its proposal that part of its work would be sub-contracted to two sub-contractors. Both of them are companies within the same group of companies as the contractor, and possess the skills and experience in image processing and development of large-scale projects. One sub-contractor is a company registered locally and the other is a Shenzhen-based company. The other two contractors do not have any sub-contractor.

The OGCIO will implement the relevant security measures to protect users' personal data and ensure system security, in accordance with the government IT security policy and guidelines and the Personal Data (Privacy) Ordinance. Such measures include:

(i) personal data in the eID system will be encrypted and stored on the government cloud platform in the government data centre. The data will not be transmitted outside Hong Kong;

(ii) the contractors and sub-contractors will only use test data not containing any personal data during development and maintenance of the eID system, which will only be carried out in the development and testing environments. Therefore they will not have access to any personal data of residents; and

(iii) privacy impact assessments, privacy compliance audits, and information security risk assessments and audits will be conducted by independent third parties.

(4) eID itself will not store any personal data. Personal data provided during eID user registration will only be used by OGCIO staff for account management and identity verification for the eID system. The data will be encrypted using prevailing internationally recognised standards (Advanced Encryption Standard) and will be stored in government data centre facilities only. In conformance with industry encryption standards, Transport Layer Security will also be adopted to encrypt data to ensure security and integrity of the data transmitted over the Internet.

The contractors and sub-contractors will not have access to any personal data of residents during development and maintenance of the eID system.

The development and operation of the eID system will adopt the information security management system (ISO/IEC 27001) and measures set out by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), which include the establishment and stringent enforcement of data access rights for all personnel to prevent any unauthorised access to personal data.

(5) Any organisation adopting eID is required to comply with the information security and related technical requirements set out in the terms of use of eID, and can do so only by making use of the application programming interfaces provided by the OGCIO and after verification of server certificates. No other personnel or other means can connect to the eID system. Data will also be encrypted during transmission to ensure security.

Personal data collected during eID user registration will only be used by the eID system for account management and identity verification. Any government department or public organisation that needs to use personal data of an eID user (such as for form pre-filling) must obtain his prior consent in accordance with the Personal Data (Privacy) Ordinance.

(6) In October 2018, the OGCIO consulted the Office of the Privacy

Commissioner for Personal Data on the design and operation of the eID system, and will seek its professional advice on various issues during the system development stage. The OGCIO has also engaged independent third parties to conduct privacy impact assessment and information security risk assessment and audit shortly. The OGCIO will ensure that the eID system complies with the provisions of the Personal Data (Privacy) Ordinance as well as the government IT security policy and guidelines. The relevant advice and information of the assessment reports can be provided to the Legislative Council provided that such disclosure will not pose security risks to the system.