DRAFT

LC Paper No. CB(1)1692/07-08(01)

(Translation)

"Subject to the actual answer given at the Council Meeting"

LegCo Question No. 1
(Oral Reply)

Asked by: Hon TSANG Yok-sing Date of Meeting: 28 May 2008

Replied by: Secretary for Commerce and Economic Development

Question

Regarding the leakage of personal data of the public by government departments and public organizations, will the Government inform this Council:

(a) of the total number of such cases in the past three years and the number of people whose data were involved in those cases; among such cases, the number of those in which the authorities concerned had informed the Police, the Office of the Privacy Commissioner for Personal Data and the people affected about the leakage;

(b) whether various government departments and public organizations have issued to their staff guidelines, stipulating the restrictions on the access, downloading, copying and sending of personal data of members of the public through computers and their accessories (such as USB memory sticks and card readers), security standards and procedure on reporting loss of data; if they have, of the contents of such guidelines; if not, whether such guidelines will be issued; and

(c) whether various government departments and public organizations have plans to review the existing information security measures and systems, and enhance staff awareness of information security; if they have, of the details; if not, the reasons for that?

Q1

Reply

Madam President,

Regarding the questions raised by the Hon TSANG Yok-sing, my reply is as follows:

(a) In the past three years, the Government received 14 reports up to 25 May 2008 in connection to the leakage of personal data involving around 1,900 citizens by government departments. For the same period, there were 16 cases of information leakage by public organizations involving about 44,000 citizens. At present, data users are not required to report leakage of personal data to the Privacy Commissioner under the Privacy Data (Protection) Ordinance. However, the Government has issued internal guidelines to departments requiring them to report information leakage incidents to the central incident response office. Of the above 30 cases, 7 government departments and public organizations had notified the Police, Privacy Commissioner and affected citizens. For the other 23 cases (which might involve crimes like theft or without the persons' contact information), the concerned government departments and public organizations had suitably reported to the relevant parties.

(b) Government has developed a comprehensive set of information security regulations and policies and has promulgated these to B/Ds. These regulations, policies and associated procedures and guidelines

Q1

were developed with reference to international best practices and are reviewed from time to time to reflect changes in technology and security threats. The topics covered include access control to information systems and data, physical security, software asset management and authorization requirements for using software not supplied by Government. B/Ds are also required to periodically remind their staff including contract staff about the need to comply with information security provisions and provide training to them where necessary.

For public bodies, B/Ds who have purview over them will take into account the government security regulations and policies in their respective regulatory or administrative arrangements with the public bodies. Public bodies are generally recommended to adopt or customise government information security related policies, guidelines and technical information when formulating their own information security policy, programme plans and implementation.

In case security incidents do occur, individual B/Ds are responsible for conducting initial investigations in the first instance. They are required to report the incidents to a central incident response office if the incident involves personal data or classified information, and/or affects public services or the Government.

For public bodies, I understand they will deal with the incidents in accordance with any applicable legislation or regulations and will consider making public announcements depending on the

Q1

circumstances of the individual case.

(c) When B/Ds undertake system development projects, OGCIO requires and facilitates the conduct of Privacy Impact Assessments and Security Impact Assessments. B/Ds are also required to carry out security risk assessment of their information systems at least once every two years.

While the investigations for some of these incidents are still in progress, the preliminary findings are that most of the incidents are caused by lack of awareness and/or alertness of the established information security regulations, policies and guidelines especially on the use of portable electronic devices and the file sharing software. As an immediate measure, two reminders have been issued to all Government staff (and contract staff?) about their obligations to protect government information systems and classified/personal data in accordance with standing guidelines and requirements. To further enhance staff awareness of and facilitate their compliance with information security requirements, OGCIO and SB with the support by Civil Service Bureau are working closely with departmental IT security officers to design a communication programme to impress upon all staff the importance attached by the Government on information security and data privacy, and to build and sustain a high level of awareness, vigilance and commitment among all staff. The handling of official documents outside the office, or from home, will be a particular area of focus in these

programmes.

On the governance side, the Government has established mechanisms for reviewing our information security management framework and measures to facilitate compliance by B/Ds. The OGCIO and SB play a leading role in this, with participation by other administrative and law enforcement agencies on a need basis. The Government will review the information security policies, guidelines and facilitation measures in the next 3 to 4 months addressing these recent issues.

For public bodies, again B/Ds who have purview over them are expected to convey the latest development in the Government for their adoption and/or reference.