立法會
Legislative Council

LC Paper No. CB(1)2311/07-08
(These minutes have been seen by the Administration)

Ref : CB1/PL/ITB/1

Panel on Information Technology and Broadcasting

Minutes of special meeting
held on Friday, 30 May 2008, at 8:30 am
in the Chamber of the Legislative Council Building

Members present	**:**	Hon Albert Jinghan CHENG, JP (Chairman) Dr Hon David LI Kwok-po, GBM, GBS, JP Hon Fred LI Wah-ming, JP Dr Hon LUI Ming-wah, SBS, JP Hon Bernard CHAN, GBS, JP Hon Howard YOUNG, SBS, JP Hon Emily LAU Wai-hing, JP
Members attending	**:**	Hon James TO Kun-sun Hon LAU Kong-wah, JP Hon Audrey EU Yuet-mee, SC, JP Hon WONG Kwok-hing, MH Dr Hon KWOK Ka-ki
Members absent	**:**	Hon SIN Chung-kai, SBS, JP (Deputy Chairman) Dr Hon Philip WONG Yu-hong, GBS Hon Jasper TSANG Yok-sing, GBS, JP Hon Timothy FOK Tsun-ting, GBS, JP Hon Albert CHAN Wai-yip Hon Ronny TONG Ka-wah, SC
Public officers attending	**:**	Ms Mimi LEE Deputy Secretary for the Civil Service 3

Miss Gloria LO
Principal Assistant Secretary for Food and Health (Health)

Mr Jeremy GODFREY
Government Chief Information Officer
Office of the Government Chief Information Officer

Mr John WONG
Assistant Government Chief Information Officer (Infrastructure & Security)
Office of the Government Chief Information Officer

Dr Heston KWONG
Assistant Director (Special Health Services)
Department of Health

Mrs KWAN CHAN Suet Mui
Assistant Director (Information Systems)
Immigration Department

Mr Michael Brian DOWIE
Director of Management Services
Hong Kong Police Force

Mr Austin KERRIGAN
Assistant Commissioner of Police (Support)
Hong Kong Police Force

Attendance by invitation : Hospital Authority

Ms Nancy TSE
Director (Finance)

Dr P Y LEUNG
Director (Quality & Safety)

Dr N T CHEUNG
Chief Medical Informatics Officer

Dr Libby LEE
Deputising Chief Manager (Patient Safety & Risk Management)

Office of the Privacy Commissioner for Personal Data, Hong Kong

Mr Roderick B WOO, JP
Privacy Commissioner for Personal Data

Ms Brenda KWOK
Chief Legal Counsel

Ms Margaret CHIU
Legal Counsel

Clerk in attendance : Ms YUE Tin-po
Chief Council Secretary (1)3

Staff in attendance : Ms Annette LAM
Senior Council Secretary (1)3

Ms May LEUNG
Legislative Assistant (1)6

Action

I. Issues relating to the recent losses of portable electronic storage devices containing personal data held by government departments/public hospitals and online leakage of confidential information held by the Immigration Department

(LC Paper No. CB(1)1679/07-08(01) -- Paper provided by the Administration

LC Paper No. CB(1)1679/07-08(02) -- Paper provided by the Hospital Authority

LC Paper No. CB(1)1679/07-08(03) (Chinese version only) -- Draft Hansard on oral question no. 4 raised by Hon Audrey EU Yuet-mee on "Protection of personal data" at the Council meeting on 21 May 2008

LC Paper No. CB(1)1679/07-08(04) -- Written question no. 15 raised by Hon Emily LAU Wai-hing on "Review of the Personal Data (Privacy) Ordinance" at the Council meeting on 21 May 2008 and the Administration's reply

LC Paper No. CB(1)1679/07-08(05)	--	Written question no. 19 raised by Hon CHEUNG Hok-ming on "Loss of patient data stored in electronic devices" at the Council meeting on 21 May 2008 and the Administration's reply
LC Paper No. CB(1)1692/07-08(01)	--	Oral question no. 1 raised by Hon Jasper TSANG Yok-sing on "Protection of personal data by government departments and public organizations" at the Council meeting on 28 May 2008 and the Administration's reply
LC Paper No. CB(1)1679/07-08(06) (English version only)	--	Letter dated 7 May 2008 from Hon SIN Chung-kai
LC Paper No. CB(1)1692/07-08(02)	--	Relevant newspaper cuttings on 27 May 2008
LC Paper No. CB(1)1704/07-08(01) (Chinese version only)	--	Relevant newspaper cuttings on 28 May 2008
LC Paper No. CB(1)1741/07-08(01) *(tabled at the meeting and subsequently issued on 2 June 2008)*	--	Speaking note of the Government Chief Information Officer)

Welcoming remarks by the Chairman

The Chairman welcomed the Privacy Commissioner for Personal Data (PCPD) and representatives of the Administration and the Hospital Authority (HA) to the meeting. He then invited representatives of the Office of the Government Chief Information Officer (OGCIO), HA, and those bureaux and departments involved in the recent data leakage incidents to brief members on the background to such incidents and improvement measures taken.

Briefings by the Administration, the Hospital Authority and the Office of the Privacy Commissioner for Personal Data

Office of the Government Chief Information Officer

2. The Government Chief Information Officer (GCIO) said that the recent data leakage incidents were most regrettable and he would like to take the opportunity to apologize to the public. He informed members that it had just come to light that an officer of the Food and Environmental Hygiene Department (FEHD) had inadvertently sent an email to a complainant with an attachment

containing sick leave records of 170 FEHD staff. He then briefly reported on the cases of lost or stolen portable electronic storage devices containing identifiable personal data held by the Civil Service Bureau (CSB), Department of Health (HD) and HA, as well as the online leakage of confidential information held by the Immigration Department (ImmD) and the Hong Kong Police Force (the Police). Reports had been made to PCPD in respect of all these incidents. Investigations to date found that no departmental core systems or communications networks had been compromised. In all cases (except the ImmD case which involved mostly visitor-related information with no contact details), data subjects whose personal data were compromised had been informed of and advised on any extra care they should take to guard against possible misuse of their data. GCIO said that many of the data leakage incidents were due to a lack of staff awareness of the security regulations and knowledge of compliance, as well as lack of understanding of the risk of compromising personal data. Following the incidents, the bureaux and departments concerned had taken steps to tighten the relevant security procedures and reminded staff of the security requirements. Computer software and hardware were also made available for staff to work securely. GCIO then outlined the measures taken and the enhancement programmes to be implemented by the OGCIO and bureaux/departments in reducing risk of further leakage and addressing human and management issues identified. The details were set out in the Administration's paper (LC Paper No. CB(1)1679/07-08(01)).

The Hospital Authority

3. Director (Finance) of HA (D(F)/HA) apologized for the leakage of patient data and briefed members on HA's existing policies and guidelines on data protection, security and access control of HA's IT system, the promulgation of guidelines and staff training, as well as improvement measures that had been taken to enhance protection of patient data, details of which were set out in LC Paper No. CB(1)1679/07-08(02).

4. D(F)/HA advised that HA had set up a Task Force on Patient Data Security and Privacy (Task Force) to review its existing policies and security system on patient data protection and to recommend improvement measures. The Task Force would complete its work and submit a report to HA's Chief Executive in three months' time.

The Immigration Department

5. The Assistant Director (Information Systems) of the Immigration Department (AD(IS)/ImmD) briefed members on the recent data leakage on the Internet and highlighted the following points:

(a) concerning the leakage of information caused by a new Immigration Officer who had copied some files containing identifiable personal data to his computer at home, preliminary investigations had completed and the incident was reported to PCPD;

(b) no USB connectivity was provided in the design of the Department's application system. All documents and personal data could not be downloaded or posted on the Internet. Staff used to work overtime at the office instead of taking work home;

(c) immediate actions had been taken to remove relevant file documents and file sharing applications and reformat the hard disc of the concerned officer's computer at home. The Department's computer workstations were checked to ensure no unauthorized software was installed; and

(d) after the incident, all staff were immediately reminded verbally and the relevant security guidelines and regulations on data protection and the proper handling of personal data were circulated. On-going efforts would be made to raise the vigilance of all staff in this respect.

The Department of Health

6. The Assistant Director (Special Health Services) of the Department of Health (AD(SPH)/DH) briefed members on the incident and follow-up actions taken by DH, as summarized below:

(a) the loss of a portable USB drive by a Medical and Health Officer of the Tuen Mun Child Assessment Centre which contained working files and personal data of 668 patients was reported to the Police and PCPD on 22 and 25 April 2008 respectively. DH had informed the affected children and their families in writing on 24 April 2008 advising them to stay alert to any possible abuse of their data. A press conference was held on 25 April 2008 to make a public apology and announce follow-up actions on the incident. A telephone hotline was also set up to handle public enquiries in this respect;

(b) standing circulars on the use of removable data storage devices for computers and IT system were updated. Staff members were reminded not to store identifiable personal data in such devices unless under exceptional circumstances and with the approval of the respective service heads. Private data and information stored in such devices must be encrypted and kept to a minimum that was essential for operational needs, and should be erased immediately after use; and

(c) seminars on data protection and office security targeting department heads, executive staff and IT security staff were held to enhance staff awareness.

The Police

7. The Director of Management Services of the Police (DMS/Police) said that the Police took a very serious view of the leakage of documents containing sensitive operational information and personal data of 19 subjects on the Internet through Foxy, a peer-to-peer file sharing application. He apologized for the leakage and briefed members on the following:

(a) investigations found that the leakage on the Internet was due to individual officers' failure to comply with the relevant Police General Orders on information security and the protection of personal data. There was no evidence to suggest that the Police IT system had been compromised;

(b) relevant guidelines were circulated and briefing sessions were held to remind staff of the importance of information security and the potential risk of using file sharing applications. According to the instructions given on 27 May 2008, all staff members had been advised to remove police information from their personal computers by early June 2008. They would also be reminded of the dangers of the use of Foxy file sharing application; and

(c) a working group was set up under the Deputy Commissioner of Operations to conduct an overall review of IT security, and to examine the sufficiency of office computers as well as the use of personal computers for work at home.

The Civil Service Bureau

8. The Deputy Secretary for the Civil Service 3 of the Civil Service Bureau (DS(3)/CSB) briefed members on the data leakage incident involving disciplinary cases and the remedial actions taken as summarized below:

(a) a portable electronic storage device containing information on two disciplinary inquiries involving the names and titles of 25 serving civil servants was found missing on 23 April 2008. The loss was reported to the Police and PCPD. Apologies were conveyed to all 25 civil servants concerned;

(b) the officer responsible for the loss of data had been warned following the investigation;

(c) security measures on the use and safe-keeping of portable electronic storage devices containing personal or classified data were reviewed and stepped up. Staff were reminded through briefings and circulars to observe relevant guidelines and regulations at all times; and

(d) staff were reminded not to use portable electronic storage devices to download, store or transmit classified data. They were also advised that under no circumstances should any classified data be brought home. If there was a genuine need to do so, staff should seek prior approval and only use devices with appropriate security protection provided by CSB. If necessary, a Virtual Private Network (VNP) notebook computer using a secure network with encryption and authentication features could be provided centrally for use.

The Office of the Privacy Commissioner for Personal Data

9. PCPD said that his office was responsible for overseeing the enforcement of the Personal Data (Privacy) Ordinance (PDPO) (Cap. 486) covering both the private and public sectors, including public bodies. Compliance with PDPO was the responsibility of every citizen and data user, including civil servants. In this connection, he pointed out that the Administration's Paper (LC Paper No. CB(1)1679/07-08(01)) shown that not until the outbreak of the data leakage incidents, the OGCIO had not taken active steps to remind all Government staff of the obligation to comply with the requirements of the PDPO. The data leakage reporting arrangement was only announced by the Administration for the first time in its circular issued on 8 May 2008. As such, PCPD questioned the determination and commitment of the Administration in promoting compliance with PDPO.

Discussion

Notifying data subjects affected by the data leakage incidents

10. Ms Emily LAU expressed disappointment about the recent data leakage incidents involving a number of government bureaux and departments as well as the Hong Kong and Shanghai Banking Corporation (HSBC) which had raised much alarm in the community. She was also gravely concerned about the possible serious consequences that could cause to the data subjects because of the sensitive operational details leaked by the Police on the Internet. She enquired whether all persons affected in the leakage incidents had been notified and whether the bureaux and departments as well as public bodies concerned would commit themselves to be responsible for any loss suffered by the affected data subjects arising from the incidents, as in the case of HSBC.

11. D(F)/HA, AD(SHS)/DH and DS3/CSB responded that all the data subjects involved in the recent incidents had been informed of the leakage and advised to be vigilant to any possible misuse of their data. In the case of the ImmD, AD(IS)/ImmD said that of the 14 persons affected, 11 were visitors and three were local residents for whom there was no sufficient contact information for follow-up. Persons affected by the leakage, if considered necessary, could lodge a claim in writing to ImmD. DMS/Police said that as directed by the Commissioner of Police, actions were being taken to notify the persons affected in the leakage. A total of 19 data subjects were involved in the four documents exposed on the

Internet. As the documents did not contain sufficient details, it would take some time to identify the persons concerned.

12. Mr LAU Kong-wah noted that of the 30 leakage incidents in the past three years involving some 44 000 data subjects, only seven government departments and public organizations had notified the affected citizens. He expressed concern about the selective notification to affected citizens and the lack of a standard practice among bureaux and departments to alert data subjects affected by the leakage.

13. GCIO replied that individual bureau and department would decide whether data subjects concerned should be notified on a case by case basis. The question of whether it should be a mandatory practice to notify affected data subjects of the leakage and whether exceptional circumstances could warrant special consideration would be examined in the coming review.

14. On compensation to the persons affected by the leakage, PCPD advised that data subjects whose personal data were compromised could seek damages through civil proceedings. He said that at present, there were no statutory provisions or resources for PCPD's office to assist data subjects in claiming damages.

Disciplinary actions against staff causing the data leakage

15. Mr WONG Kwok-hing expressed disappointment that the secretaries of various bureaux did not attend this meeting to respond to concerns raised by the public and by members about the data leakage involving departments/public bodies under their purview. He requested the Administration and HA to give an account on how cases of abuse of personal data had been dealt with and whether disciplinary actions had been taken against those staff who had not complied with the departmental guidelines. He also enquired about measures to safeguard privacy and protect personal data.

16. Sharing Mr WONG's view, Ms Emily LAU called for an independent investigation into the leakage incidents with a view to recommending comprehensive improvement measures to prevent recurrences.

17. DS3/CSB responded that the Administration was gravely concerned about any leakage of personal data. The departments/institutions involved in the data leakage had either completed or were making thorough investigations into the incidents. She assured members that any breaches and non-compliance would be dealt with in accordance with the established disciplinary mechanism of the civil service following the investigations. D(F)/HA confirmed that the data leakage incidents were under investigation. Appropriate actions would be taken in accordance with prevailing Human Resources Policies against breaches of the established security guidelines and personnel policies.

18. DMS/Police informed members that the cases in question had been referred to the Technology Crime Division in the Commercial Crime Bureau for full

investigations. Disciplinary proceedings would be instituted as appropriate for cases that did not involve criminal element. Disciplinary action would be taken in accordance with established procedures if any officers were found to have breached the Police internal guidelines. Penalties would range from advice to dismissal, depending on the nature and seriousness of the breaches.

Monitoring file sharing applications

19. In response to Mr James TO's enquiry about the monitoring of file sharing applications, AD(IS)/ImmD replied that risk assessment and internal security audits were regularly conducted on the department's IT system. ImmD had been closely monitoring the situation to see if any classified information of the department could be found through the search engine of a file sharing application on the Internet.

20. DMS/Police advised that cyber patrols were conducted to monitor the Foxy and other peer-to-peer file sharing applications to uncover any classified documents circulating on the Internet. Immediate action would be taken to remove such documents. He nevertheless pointed out that such documents once passed onto other parties would be difficult to erase totally.

21. GCIO supplemented that a security team would monitor the Internet daily to search for government documents circulating on the Internet that might be shared by common forms of software.

Adopting advanced data protection technologies

22. Given the convenience and the popular use of the Internet and portable electronic storage devices, Mr Howard YOUNG considered that instead of prohibiting the use of such devices and banning take-home work, educational efforts should be stepped up to enhance staff awareness of information security and their knowledge on the secure use of such devices. Citing the auto-shut-down of net banking as an example, he suggested deploying state-of-the-art data protection technologies to facilitate and enable staff to work in a secure computing environment.

23. Mr LAU Kong-wah sought information on concrete measures to be adopted in preventing further leakage to restore public confidence in the handling of personal data by the Government.

24. GCIO responded that working at home had been a particular source of risk in recent incidents. In order to enable authorized government officials to work outside the office for operational needs, technological solutions had been deployed. These included advanced USB flash drives with encryption and password lockdown (used in HA), virtual private network (VPN) notebook computers using a secure network with encryption and authentication features (used in CSB), and application software with security features and access control. On peer-to-peer Foxy file sharing application, GCIO said that while IT asset management techniques could help ensure that no unauthorized application software was loaded

onto a Government information system or prevent any unauthorized information system device from being connected to a Government information system, it was difficult to stop the related staff from installing such software at home computers. It was therefore a general rule that staff were advised not to copy or take home any official files containing classified and personal data. Given that most of the recent incidents were caused by such unauthorized act at home, all bureaux and departments were advised to examine the risk and implication of such act. Bureaux and departments were also advised to take appropriate measures to reduce the risk and make sure that staff authorized to work at home was provided with a secure computing environment.

25. GCIO, however, stressed that there was a limit to what technology and procedures could achieve and that no technological means could ever guarantee 100% data protection. Since many security threats in the computing environment were attributable to human factors, training and educational programmes would be stepped up to foster a culture and commitment to data protection as well as to enhance staff awareness of security issues and their knowledge on how to comply with the relevant information security requirements. OGCIO and the Security Bureau with the support of CSB were working closely with departmental IT security officers to design a communication programme to build and sustain a high level of awareness, vigilance and commitment among all staff on the handling of official documents outside the office and/or working at home.

26. Chief Medical Informatics Officer of HA (CMIO/HA) advised that HA's patient information system had been upgraded in view of the recent cases of loss of portable electronic storage device. The downloaded patient data with identifiable patient and personal information would also be protected through encryption. In addition, mandatory use of advanced USB flash drives with encryption and password "lockdown" had been introduced for protecting patient data.

Review of information security policies and regulations

27. GCIO advised that the Administration would review information security policies and regulations, the content of security audits, and the roles and responsibilities for assuring information security throughout the public sector in the next three to four months in the light of the findings of investigations into the incidents. The Administration would also provide guidance to bureaux and departments as well as public bodies, and request them to put in place their own data protection measures in accordance with the guidance and the provisions in PDPO, having regard to their specific operational needs.

28. The Chairman enquired what security guidelines and measures were in place to safeguard against storing personal data for private use by officers leaving the service. GCIO responded that this would be an abuse of personal data which contravened PDPO and the security guidelines in the civil service/public bodies, and enforcement and disciplinary action would be instituted in such cases. Assistant Government Chief Information Officer (Infrastructure &Security) advised that all government officers were required to erase the data from their personal

computers immediately after use, and bureaux and departments should be responsible for monitoring staff compliance. D(F)/HA said that established guidelines on the security and disposal of storage media, and personnel procedures were in place requiring out-going staff to return any office assets, including data in their possession. DS(3)/CSB said that in accordance with the requirements under the data protection principles, a time limit had been set for the retention of personal data relating to staff recruitment and appointment. PCPD pointed out that breaches of the data protection principles of the PDPO and improper use of data for personal gain were not criminal offences. Recommendations had been made to the Administration for conducting a public consultation on introducing amendments to the PDPO, including making it a criminal offence for any person to obtain, disclose or sell personal data held by a data user without the data subjects' consent.

Powers and functions of Privacy Commissioner of Personal Data

29. In response to PCPD's question on the Administration's commitment to promoting compliance with PDPO, GCIO replied that compliance with the statutory requirements of PDPO was the responsibility of every data user, including the Government and non-government institutions. He stressed that the Government attached great importance to the security requirements and the data protection principles of PDPO. In this respect, a circular had been issued on 8 May 2008 to all Government staff reiterating their obligations to observe the requirements under PDPO. References to PDPO were also made in the Baseline IT Security Policy issued by the OGCIO. DS3/CSB added that CSB had issued in August 2002 detailed guidelines on compliance with PDPO on employment related personal data. In fact, a number of circulars had been issued by the Government to all bureaux and departments explaining the provisions of PDPO to ensure their compliance with such legislation.

30. Mr WONG Kwok-hing expressed disappointment that PCPD's office seemed to be a "toothless tiger" without power. Sharing Mr WONG's view, Dr KWOK Ka-ki expressed concern that PCPD's office, being a statutory body funded by the Government to safeguard personal data security and protection, had to rely on media reports to obtain information on data leakage incidents. Mr LAU Kong-wah said that apart from acting upon complaints, PCPD's office was empowered by the PDPO to proactively initiate investigations into any alleged data leakage. In this connection, Mr WONG Kwok-hing, Mr KWOK Ka-ki and Mr LAU Kong-wah sought information on the measures and actions taken/to be taken by PCPD to protect privacy and data security.

31. In response, PCPD said that his office, with only 39 staff, did not have sufficient resources to monitor all set-ups and forestall any possible leakage in advance. PCPD's office had so far only received one complaint concerning the case of the United Christian Hospital (UCH) where an employee lost a USB flash drive containing data on 26 patients. No complaints about data loss at other hospitals, public bodies, bureaux and departments had been received by his office. He stressed that his office had, within its capacity, taken prompt actions on data leakages once they came to light in the media. Apart from the UCH incident

which was under investigation, he had decided to take the unprecedented step of exercising the inspection power under PDPO to inspect the personal data systems of public hospitals. PCPD's office had also initiated compliance checks including investigations into the recent data leakage involving a number of public hospitals and clinics, DH, ImmD, CSB and the Police and also the HSBC's case involving the loss of a computer server containing customer data while the office was under renovation. Reports and recommendations would be published on completion of investigations.

32. On education and training, PCPD highlighted that his office had done its best within the limited provision of $640,000 allocated for promotion and education. From 2007 till now, a total of 17 seminars had been conducted for the public and 93 talks organized for institutions (including HA) and they were well attended by more than 10,000 participants. However, despite an additional funding of $1 million for 2008-2009, the provision could barely be enough for the production of an API. If more resources were given, his office would be able to embark on more preventive educational and training programmes on data protection and security.

33. PCPD further pointed out that the extent of PCPD's power as prescribed by PDPO was determined by legislators when PDPO was enacted 12 years ago. His office could only come to know about the leakages through media enquiries and reports, as presently there was no statutory requirements for data users to report leakages of personal data to his office. He called on the Administration to seriously consider making it a good practice among government departments to report such incidents to his office for timely follow-up. As his office had earlier recommended amendments to PDPO to the Constitutional and Mainland Affairs Bureau, he called on the Legislative Council Members to support expanding PCPD's power in the coming PDPO review. In this connection, GCIO said that the Administration would consider whether the practice of reporting data leakage incidents to PCPD should be made mandatory.

Staff taking work home

34. Mr James TO enquired whether ImmD and the Police had ever assessed the extent to which their staff were taking confidential/classified documents home to work after office. He sought clarification whether staff of ImmD could download such documents from the Department's IT system.

35. In response, AD(IS)/ImmD advised that ImmD's IT system on entry/exit records and personal data had no outside connectivity and therefore files/documents could not be downloaded or posted on the Internet. She stressed that it was the Department's established policy that except under exceptional circumstances and with prior approval, no classified documents and files should be taken out of the office. Staff members generally preferred to work overtime in the office and no staff had requested taking home documents with personal data to work because of the bulk of files they had to make reference to. Relevant guidelines, regulations and instructions on information security and protection of personal data were

circulated regularly to staff members to enhance their awareness. To ensure a secure computing environment, notebook computers with encryption and authentication features would be provided for staff members authorized to work at home for operational reasons.

36. Referring to the enhanced security devices such as advanced USB flash drives with encryption, password "lockdown" and VPN notebook computers used by HA and CSB, Mr James TO enquired whether the Police would make similar arrangements for its staff pending the Working Group's review.

37. DMS/Police responded that a number of interim measures had been introduced pending the outcome of the overall review of IT security. This included a major exercise to ensure that every staff member would be personally briefed to remove police information from their personal computers, and alerted to the dangers of peer-to-peer file sharing applications. On the provision of computer facilities, DMS/Police advised that the Police currently had over 13 300 computers of which 9 736 computers were networked. Computers were allocated to officers at inspector rank and above and also to junior officers with operational needs. There were also terminals for shared use. He highlighted that the number of computers had increased from 7 000 to more than 9 000 over the past two years. The management would review the sufficiency of computers for use by staff members, and continue to upgrade and increase the provision of computers where resources permitted and with a justified need. Efforts would also be made to assess the extent and examine the reasons for taking work home.

38. Mr LAU Kong-wah opined that it was unfair and irresponsible to put all the blame of the data leakage on frontline staff. Referring to the case of the Police where 200 frontline police officers had to share four computers in a police station, he pointed out that there was a practicable need for officers to bring work home given the heavy workload and inadequate resources. He considered the data leakage incidents a dereliction of duty on the part of the Police. The management should check and monitor the use of classified documents and alert their staff to the potential danger of peer-to-peer file sharing applications. Mr LAU enquired what immediate improvement measures would be implemented to reduce the risk of further leakage. He also urged for a comprehensive review on the use of personal computers at home for office work.

39. DMS/Police said that different types of policing work involved varying needs on computers. As the majority of the officers performed frontline and non-desk-based duties, higher priority to use computers would be accorded to certain officers. While officers of inspector rank and above as well as junior officers with operational needs had designated computer terminals, the other officers had access to common terminals. Moreover, there were no requirements for reports/statements to be prepared using word processing software, as hand-written reports/statements would suffice. He stressed that in the coming review, the management would examine the reasons for taking work home, assess whether there was a real need to do so, and review whether taking work home was due to insufficient number of office computers or due to individual officer's work

habits. He highlighted that the management had taken note of officers' need for computers. In fact, the number of computers had increased steadily over recent years. Where resources permitted and the need justified, the Police would continue to make its best effort to make sufficient number of computers available for staff use. At members' request, DMS/Police agreed to report to the Panel in due course the improvement measures implemented.

40. GCIO agreed that the management, to a certain extent, should also be responsible for the data leakage. Given that most of the recent incidents were caused by officers working at home without authorization, efforts would be made to address the human and management issues leading to such leakage, and to step up enforcement and strengthen internal management to ensure compliance with the relevant security regulations and guidelines. In this connection, all bureaux and departments had been requested to look into the matter, and advise their staff not to bring classified data home. Bureaux/departments should also make sure that officers authorized to work at home were provided with a secure computing environment.

41. Dr KWOK Ka-ki noted that apart from long hours of bedside service in hospitals, the additional workload on research and data compilation had forced many hospital staff to take work home. He enquired about the HA's annual budget on IT security and sought details of the IT support and training on data protection and IT security provided for hospital staff.

42. In response, D(F)/HA said that IT security was part and parcel of the HA IT/IS infrastructure to support the clinical management operational systems. It would be difficult to just isolate the budget for IT security. However, the IT budget which included recurrent and development expenditure for IT services provision accounted for about 1.6% - 1.7% of the HA total budget. She highlighted that HA had all along implemented a secured network infrastructure comprising firewalls, intrusion protection and URL-filtering systems for safeguarding personal data from unauthorized access and malicious attacks. Following the leakage, HA's patient information system had been upgraded and patient data downloaded would be automatically encrypted. The use of advanced USB flash drives with encryption and password "lockdown" had also been introduced. On the provision of IT facilities, she said that HA's some 20 000 computers were sufficient for staff use. Information security policy guidelines had been promulgated to frontline staff through circulars, newsletters, booklets, HA intranet, seminars and briefings on information technology for hospital staff well before the incidents came to light. For new employees, in particular hospital staff, patient information confidentiality and IT security were included in the orientation programme. Patient confidentiality and data access controls were also included in the training programme for intern doctors on the use of HA's clinical system. Following the incidents, Operational Circulars on "Enhanced Measures on Enforcing Personal Data Security" and "Policy on the Management of Loss of Electronic Devices Concerning Patient Identifiable Personal Data" had been issued to remind staff of the importance of data security. A promotional video and refresher education programmes had been launched to educate HA staff on patient

data protection. Each hospital cluster had an IT Committee which was responsible for IT matters and would provide support to staff. D(F)/HA stressed that the management would endeavour to provide the necessary IT support to staff.

43. Dr KWOK Ka-ki said that the IT Committee did not have any funding since it was mainly made up of volunteers. He opined that the management should provide staff with training courses as well as face to face support and advice.

Admin

44. Dr KWOK Ka-ki and Ms Emily LAU requested OGCIO to coordinate a reply from various bureaux and departments and public bodies/tertiary institutions under their purview, setting out in a table format summary of data leakage incidents over the past three years. OGCIO should also apprise the Panel of the number of data subjects affected, whether the affected citizens/PCPD/the Police were notified, and the reasons for not informing the related parties.

(*Post-meeting note*: A summary of incidents involving leakage of personal data over the past three years provided by the Administration had been circulated to members vide LC paper No. CB(1)1875/07-08 issued on 13 June 2008. According to the summary, among 24 out of the 30 incidents, concerned government departments and public organizations had notified the affected citizens. For those cases which citizens were not notified, the main reason was due to insufficient contact information.)

45. Ms Emily LAU enquired whether the Administration had any policy on staff taking work home. She said that she personally was against the practice but if taking work home was necessary for operational reason, the Administration/management should set out clear guidelines, put in place measures to provide a secure computing environment for staff to do so, and ensure safe transit of data between home and office.

46. GCIO said that each bureau and department would have to decide its own policy and arrangements for working at home according to its own operational requirements. He however pointed out that the use of personal computers at home for office work and the transfer of data between office and home in removable storage devices posed a clear risk of data leakage. If working at home was permitted, a better way of managing security risk was to provide a secure network connection on an VPN platform, which was similar to the arrangement made in ImmD and OGCIO, so that there was no need for data download on removable storage devices. GCIO added that personal and sensitive data, if stored in removable USB drives, must be encrypted. Meetings would be arranged to brief heads of departments and requiring them to review their arrangements for working at home to minimize the risk of data leakage.

47. DMS/Police said that as a general rule, working at home was not encouraged. For Police Superintendents and above and those Chief Inspectors who had proven need and were authorized to work at home on operational grounds, they were provided with a secure computing environment with a link between

office and home on the VPN platform. The Police would review the policy to see whether there was a need to include also the inspector rank.

48. DS(3)/CSB said that the Administration had no policy for working-at-home and it was mainly an individual officer's practice. Staff were advised not to bring home classified data in all circumstances. If there was a genuine need to do so, staff should seek prior approval and only use devices with appropriate security protection provided by respective bureaux and departments. If necessary, a VPN notebook computer using a secure network with encryption and authentication features could be provided by the concerned bureau/department for use.

49. CMIO/HA said that according to HA's guidelines, staff were not allowed to store identifiable personal data in home computers. VPN facilities were available to staff authorized to work at home.

50. AD(SHS)/DH advised that in principle staff were not encouraged to bring classified information and sensitive data home for work. He said that the department had sufficient computers for use by staff in clinics and centres. Where necessary, notebooks with security measures would be provided for staff on trips outside office.

51. Referring to the Administration's comments that working at home was not encouraged, Mr James TO considered such comment offensive and demoralizing, and would lead to a conflict between frontline officers and the management. He opined that the leakage incidents were partly caused by the lack of resources and heavy workloads. Citing the Police as an example, he said that as junior officers did not have sufficient computers for use in the office, they were forced to take work home to complete their paper work. Given this, the officers concerned should not bear the blame alone and should instead be provided with technical assistance and a secure computing environment to work at home. He said that the problem could not be addressed by issuing additional guidelines. He urged the Police to acquire more computers with word processing function for input of classified information, and also provide staff with concrete technical support. DMS/Police noted Mr TO's suggestion.

52. In summing up, the Chairman requested government representatives to convey to bureaux secretaries members' disappointment about their non-attendance at this meeting. Ms LAU suggested and members agreed that a panel meeting be held in early July before the end of the current legislative session, and secretaries of the various bureaux involved in the data leakage would be invited to report on the progress of the follow-up actions taken and remedial measures implemented.

(*Post-meeting note*: As the Secretary for Commerce and Economic Development would not be able to attend the special meeting scheduled for 8 July 2008 and the Administration had also advised that there was no further update on issues relating to the recent personal data/classified documents leakage, the Chairman, after consultation with some Panel members, had instructed that the special meeting on 8 July 2008 would not

be held.)

II. Any other business

53. There being no other business, the meeting ended at 11:05 am.

Council Business Division 1
Legislative Council Secretariat
24 September 2008