立法會
Legislative Council

LC Paper No. CB(1)1269/08-09
(These minutes have been seen by the Administration)

Ref : CB1/PL/ITB/1

Panel on Information Technology and Broadcasting

Minutes of meeting
held on Monday, 8 December 2008, at 2:30 pm
in Conference Room A of the Legislative Council Building

Members present	**:**	Hon LEE Wing-tat (Deputy Chairman) Hon CHAN Kam-lam, SBS, JP Hon Emily LAU Wai-hing, JP Hon Timothy FOK Tsun-ting, GBS, JP Hon WONG Ting-kwong, BBS Hon Ronny TONG Ka-wah, SC Hon Cyd HO Sau-lan Hon WONG Yuk-man Hon Mrs Regina IP LAU Suk-yee, GBS, JP Hon Paul TSE Wai-chun Dr Hon Samson TAM Wai-ho, JP
Member attending	**:**	Hon James TO Kun-sun
Members absent	**:**	Hon Andrew LEUNG Kwan-yuen, SBS, JP (Chairman) Hon WONG Yung-kan, SBS, JP
Public officers attending	**:**	Agenda Item III Mr Duncan PESCOD, JP Permanent Secretary for Commerce and Economic Development (Communications and Technology)

	Ms Ida LEE Acting Deputy Secretary for Commerce and Economic Development (Communications and Technology)
	Mr HA Yung-kuen Deputy Director-General of Telecommunications
	Mr Chaucer LEUNG Head, Regulatory 2 of Office of the Telecommunications Authority
	Agenda Item IV
	Mr Duncan PESCOD, JP Permanent Secretary for Commerce and Economic Development (Communications and Technology)
	Mr Jeremy GODFREY Government Chief Information Officer Office of the Government Chief Information Officer
	Mr Stephen MAK, JP Deputy Government Chief Information Officer (Consulting & Operations) Office of the Government Chief Information Officer
	Mr John WONG Assistant Government Chief Information Officer (IT Strategy) Office of the Government Chief Information Officer
Clerk in attendance :	Ms YUE Tin-po Chief Council Secretary (1)3
Staff in attendance :	Ms Annette LAM Senior Council Secretary (1)3
	Ms Debbie SIU Legislative Assistant (1)6

Action

The Deputy Chairman chaired the meeting in the absence of the Chairman who was out of town.

I. Information paper issued since last meeting

2. Members noted that no paper had been issued since the last meeting held on 20 November 2008.

II. Date of next meeting and items for discussion

(LC Paper No. CB(1)326/08-09(01) -- List of outstanding items for discussion

LC Paper No. CB(1)326/08-09(02) -- List of follow-up actions)

3. Members noted that the next regular Panel meeting would be held on 12 January 2009 at 2:30 pm to discuss the following items proposed by the Administration:

(a) Mobile TV policy framework and auctioning of mobile TV-related spectrum; and

(b) District cyber centres.

Governance structure of the Hong Kong Internet Registration Corporation Limited

4. Mr James TO referred to his letters jointly signed by the Deputy Chairman dated 24 November and 8 December 2008 addressed to the Panel Chairman and tabled at the meeting. He said that following a consultancy study in 2006 and public consultation between 4 May and 15 June 2007 on the review of the administration of Internet domain names in Hong Kong, the Board of the Hong Kong Internet Registration Corporation Limited (HKIRC) had approved the proposed restructuring under which the number of directors would be reduced from 13 to 8 while the number of Government appointed directors would be increased from 1 to 4. The adjourned Annual General Meeting (AGM) of the HKIRC would be resumed on 15 December 2008 to effect the changes. Since the changes in the HKIRC's governance regime had serious impact on public interests, Mr TO suggested that an urgent Panel meeting be held to discuss the matter before the resumption of the adjourned AGM on 15 December 2008. As no member objected to Mr TO's suggestion, the Deputy Chairman requested the Clerk to arrange for a special meeting as soon as possible.

(*Post-meeting note*: With the concurrence of the Chairman, a special meeting had been scheduled for Thursday, 11 December 2008 at 4:30 pm to discuss the item "Governance structure of the Hong Kong Internet Registration Corporation Limited".)

III. Assignment of Available Spectrum in 1800 MHz Band for Provision of Mobile Public Services

(LC Paper No. CB(1)326/08-09(03) -- Administration's paper on assignment of the available radio spectrum in the 1800 MHz Band)

Briefing by the Administration

5. Referring to Telecommunications Authority (TA)'s statement issued on 4 July 2008, the Permanent Secretary for Commerce and Economic Development (Communications and Technology) (PSCED(CT)) briefed members on the Administration's decision in respect of the assignment of the available radio spectrum in the 1800 MHz Band for public mobile service to the incumbent Mobile Network Operators (MNOs) to allow for service expansion. He said that the decision was taken after a public consultation exercise conducted by the Office of the Telecommunications Authority (OFTA) in early 2008. In line with the Government's market driven policy and the guiding principles under the Radio Spectrum Policy Framework, the use of the relevant spectrum would be subject to the payment of Spectrum Utilization Fee (SUF), the level of which was to be determined by auction, adopting the Simultaneous Multi-round Ascending method. The Administration planned to gazette and table the amendments to the subsidiary legislation at the Legislative Council shortly. Upon completion of the negative vetting process on the subsidiary legislation, the TA would conduct the auction within the first half of 2009. Details of the SUF payment, auction arrangements, related legislative amendments required for the auction, and the timetable were set out in LC Paper No. CB(1)326/08-09(03).

Discussion

Mobile network services in country parks

6. Dr Samson TAM supported the Government's decision to waive MNOs' SUF payment for the use of radio spectrum in serving country parks and prescribed remote areas as an incentive to encourage MNOs to improve their mobile phone coverage in the countryside. He sought information on the current mobile phone coverage in country parks and the estimated saving of SUF per annum by MNOs arising from the waiver.

7. In response, the Deputy Director-General of Telecommunications (DDGT) said that the exemption policy was introduced in 2006 to encourage MNOs to improve coverage within country parks and prescribed remote areas. According to a recent Mobile Network Coverage Survey conducted along popular hiking trails, about 96% of popular walks and hiking/country trails were covered. While it was not easy to provide full coverage along the hiking trails due to the hilly terrain in country parks, OFTA would continue to encourage and facilitate MNOs in setting up additional base stations inside the country parks to improve service coverage.

Based on the long-term annual fee of about $1.45 million per MHz for the second generation mobile service, MNOs could save $29 million per annum resulting from the waiving of SUF for the use of radio spectrum within country parks.

8. The Deputy Chairman enquired whether the 96% coverage was based on the area of country parks or the length of hiking or country trails covered, and whether OFTA had liaised closely with the Agricultural, Fisheries & Conservation Department (AFCD) and other relevant departments and organizations to publicize details of the country park mobile phone coverage for public information.

9. In reply, DDGT said that the coverage figures were based on the length of the trails. To help hikers enjoy safe hiking, information on country park mobile phone coverage together with some 120 digital maps were uploaded on to OFTA's website for public reference. Public education programmes in the form of TV/radio announcements, posters and video clips were launched to enhance the public knowledge about mobile phone communications in country park areas and encourage them to plan well for hiking and outings. He highlighted that OFTA had close cooperation and liaison with the AFCD. Leaflets of mobile phone coverage in country parks were available to visitors and hiking groups at various country park management centres of the AFCD. OFTA had also participated in the annual Mountaineering Safety Promotion Day organized by the Civil Aid Service to help promote safety for hiking, the most recent one being held in October 2008.

Conclusion

10. The Deputy Chairman concluded that the Panel supported in principle the proposed auction arrangements and the related legislative amendments for the auction of the relevant radio spectrum.

IV. Information Security

(LC Paper No. CB(1)326/08-09(04) -- Administration's paper on information security

LC Paper No. CB(1)326/08-09(05) -- Paper on information security in relation to the series of personal data leakage incidents involving Government bureaux/departments and public bodies prepared by the Legislative Council Secretariat (background brief))

Presentation by the Administration

11. The Permanent Secretary for Commerce and Economic Development

(Communications and Technology) (PSCED(CT)) and the Government Chief Information Officer (GCIO) briefed members on the progress of Government's information security enhancement programmes targeting specifically at the problems identified in the series of data leakage incidents. The enhancement programmes covered four main areas, namely staff awareness and education, technical and procedural measures, security compliance audits, and the review of security regulations, policies and guidelines. Details of the various security enhancement measures were set out in the Administration's paper (LC Paper No. CB(1)326/08-09(04)).

Discussion

Staff taking work home

12. Ms Cyd HO referred to the prevalence of staff bringing confidential documents and sensitive data home for work. She was concerned that despite the use of advanced data protection technologies such as encrypted USB flash drives, the use of home computers shared by other family members would pose risk of data leakage. She enquired about the guidelines and measures to safeguard information security if working at home was necessary for operational reasons.

13. In response, GCIO said that after the data leakage incidents first came to light, the Director of Administration had issued circulars to strengthen guidance and tighten the rules on the use of USB devices. In general, storing classified documents and personal data in USB devices was not encouraged. Officers were told not to store classified information and data in USB drives and portable electronic devices unless it was operationally necessary, in which case permission should be sought from the departments/bureaux concerned. Following the issuance of the circular, there was a significant decrease in the use of USB drives for such purpose. Bureaux and departments had also been advised that if there was a regular operational need for staff to work on classified data outside office, the management should make available to these staff USB drives with encryption and password lockdown and lap-top computers with secured virtual network to ensure safe transit of data between home and office and to provide a secured computing environment for staff authorized to work at home. On the use of officers' home computers, staff had been strongly advised that it was unacceptable for personal and confidential data to be worked on home computers in view of the potential security risks of peer-to-peer file sharing applications that might have been installed in home personal computers.

14. Ms Emily LAU said that there was a general consensus that the level of information security awareness among civil servants was low. While stringent requirements had been set to tighten the control of working on sensitive data outside office environment, Ms LAU doubted whether staff would actually abide by the regulations and enquired about the measures to ensure compliance. She said that the Government should ascertain the extent of staff taking sensitive data to

work at home and draw up quantifiable yardsticks as benchmarks to measure the level of staff awareness so as to assess the effectiveness of the security enhancement measures.

15. In response, GCIO agreed that objective and quantifiable measures should be developed to chart the progress. He said that in view of the emerging security threats and risks, information security management was an on-going process that required the commitment and attention of both the management and staff. A number of initiatives on education and training, including a staff communication programme, had been launched to help raise staff awareness of protection of personal data and security issues. The Deputy Government Chief Information Officer (Consulting & Operations) (DGCIO(C&O)) added that those bureaux/departments with a substantial operational need for staff to take work home had put in place control measures and deployed advanced data protection technologies to enhance data protection. In addition to the security risk assessments carried out by individual bureaux/departments, the centrally managed security audits and inspections would also be conducted to monitor compliance.

Use of handheld communication devices in the Government

16. Referring to the popular use of handheld communication devices such as the Blackberry by some Government officials, especially senior officials, Ms Cyd HO enquired whether the Administration had put in place guidelines regulating such use to prevent classified information being stored in officers' personal communication devices which might pose risk of data leakage. Mrs Regina IP shared the view that confidential data stored in Blackberries would be compromised in the event that the Blackberry was lost or misplaced. Referring to media reports that Mr Obama, following his election as the President of the United States, could no longer sent out emails in his personal capacity, Mrs IP enquired whether the Chief Executive (CE) of the Hong Kong Special Administrative Region was also subject to the same requirement.

17. In reply, GCIO said that classified information in the Government's internal email system was not at risk on personal handheld devices. Emails containing classified information were encrypted and the content was not visible on portable devices. He said that Blackberries provided by the Government were password protected and encrypted. Moreover confidential emails/messages sent through the Government internal email system would not be passed to the Blackberry server and therefore would not show up on the Blackberry. As such, no confidential data, not even in encrypted form, would be stored in the Blackberry. There was currently no restriction on the CE on the use of email.

Disciplinary action against staff causing data leaks

18. Mrs Regina IP said that disciplinary actions and a formal record in staff performance appraisal file might be effective deterrents for civil servants who had

not exercised sufficient care and prudence in handling sensitive or personal data. She enquired how cases of abuse of personal data had been dealt with and whether disciplinary actions would be taken against those staff for security breaches and non-compliance.

19. In reply, GCIO said that Government bureaux/departments involved in the data leakage incidents had either completed or were conducting thorough investigation into the incidents. Disciplinary proceedings would be instituted in accordance with the established disciplinary mechanism against any breaches and non-compliance. Penalties would be imposed as appropriate depending on the nature and seriousness of the breaches.

Review of Personal Data Privacy Ordinance

20. Mr WONG Ting-kwong held the view that most of the recent data leakage incidents in the Government and private sector were mainly due to personal negligence and inappropriate handling by data users. He was alarmed to note that some sensitive personal data in printed form were misplaced by waste recycling companies in public areas, and enquired who should be held responsible for such leakage. He considered that all personal data, be it held by the Government or private companies, should be protected, and urged that the Personal Data Privacy Ordinance (PDPO) be reviewed as soon as practicable to ensure sufficient protection. He also enquired about the Government's stance of introducing legislation to make breaches of privacy a criminal offence.

21. In reply, GCIO and DGCIO(C&O) said that all data users in the public and private sectors were subject to the PDPO governing privacy and personal data security, and were required to take every practicable steps to avoid unauthorized disclosure of all sensitive data, either in paper or electronic form. As far as the Government was concerned, detailed guidelines governing the storing, handling, transmission and disposal of sensitive data/information were set out in the Government Security Regulations for Government staff to observe. The management of each bureau/department was responsible to ensure compliance by their staff. The security guidelines were also posted at the Government's website for public access. On the review of the PDPO, the Permanent Secretary for Commerce and Economic Development (Communications and Technology) (PSCED(CT)) advised that the ordinance was currently under review. In fact, the Office of the Privacy Commissioner for Personal Data (PCPD) had made some recommendations to the Constitutional and Mainland Affairs Bureau (CMAB) for consideration. The matter was also discussed by the Panel on Home Affairs at its meeting held on 4 July 2008.

22. Mr WONG Ting-kwong remarked that the Government should assume a more active role in driving the PDPO review instead of leaving the matter to the PCPD. Echoing Mr WONG, Ms Emily LAU said that the PDPO review should not be the sole responsibility of the CMAB and that CEDB should also participate

in the review.

23. In response, PSCED(CT) said that the review would go through the necessary consultation and legislative procedures. He assured members that the CEDB, same as other interested bureaux/departments, would forward comments to the CMAB which was the relevant policy bureau taking the lead in the overall coordination of the review.

24. Mr WONG Ting-kwong suggested that the PCPD and the data subjects affected by the leakage of sensitive and personal data should be notified of the leakage as soon as possible. In response, GCIO advised that Government regulations had been revised to the effect that whenever there was a security incident involving personal data, the bureau/department concerned was required to report the incident to both the PCPD and the Government Information Security Incident Response Office. PSCED(CT) added that whether affected data subjects would be notified of the leakage would depend on individual circumstances. While it was up to individual private companies to determine whether it was necessary to notify the victims of data leakage, public bodies involved in data leakage incidents would notify affected data subjects as far as practicable along with advice on measures to mitigate the impact of the leakage. Exception to these rules were permitted only when there was an overriding public interest consideration, in which case the approval of the head of the bureau/department concerned would have to be sought.

Resource allocation to the Office of the Privacy Commissioner of Personal Data

25. Mr WONG Yuk-man expressed regret that the summary of data leakage incidents set out in Annex 4 to the Administration's paper (LC Paper No. CB(1)326/08-09(04)) did not include cases before June 2008, some of which were serious leakages involving a watch list of the Immigration Department, sensitive police information on an undercover operation revealing the identity of an undercover agent, names and telephone numbers of a number of police officers, cautioned statements and staff performance appraisal, etc. He said that the brief descriptions of the incidents in the summary had played down the seriousness of the leakages and the extent of the problem, and was therefore misleading to the public and Legislative Council Members. He was disappointed that the Government failed to put in place effective measures to forestall the repeated leakages which had seriously compromised privacy and personal data security. Referring to some members' comments at the Panel's meeting held on 30 May 2008 that the PCPD was a "toothless tiger" without power, Mr WONG opined that the Government had not provided PCPD with the sufficient manpower and resources to discharge its statutory function of safeguarding and protecting personal data security.

26. Dr Samson TAM shared a similar view and requested the Administration to provide information on resources allocated to the PCPD for 2008-2009 financial

year and whether additional resources, in terms of funding and manpower, would be provided to enable PCPD to effectively discharge its statutory function. In this connection, Mr WONG Ting-kwong also suggested that consideration be given to providing resources to the PCPD for assisting victims of data leakage to seek damages.

27. In response, GCIO said that the Government took a serious view on every single leakage incident and would make continuous effort to put in place procedural, educational and technological measures to uphold a high level of information security in the Government to protect privacy and sensitive personal data. Noting members' concerns, PSCED(CT) undertook to relay members' views about the review of PDPO and resource allocation to the PCPD to CMAB.

(*Post-meeting note*: Members' concerns about the review of PDPO and resource allocation to the PCPD had been relayed to the CMAB. The Panel on Constitutional affairs had discussed the "Financial provision for the Office of the Privacy Commissioner for Personal Data in 2008-2009" at its meeting held on 15 December 2008.)

Security risk assessments

28. Dr Samson TAM noted that Government bureaux and departments had been asked to carry out a special risk assessment on security provisions for their staff in handling personal or sensitive data, including working outside the office environment. He enquired about the findings of the risk assessments and the improvement measures implemented to strengthen information security and data protection. He also asked whether international security standards would be adopted for system enhancement.

29. In reply, GCIO and DGCIO(C&O) informed the meeting that bureaux and departments were required, as a standard practice, to carry out security risk assessment of their information systems at least once every two years to reduce the risk of non-compliance. They would also carry out risk assessment whenever a new computer system was installed. Arising from the series of data leakage, bureaux and departments were requested to conduct, in addition to the routine risk assessment, a special risk assessment to identify reasons for non-compliance and draw up improvement measures to avert the risks and problems identified. Following the assessment conducted, individual bureau and department had implemented improvement measures in accordance to their operational needs to avert the risks identified. Some common improvement measures including security awareness promotion and training, tightening the control of work-at-home, and the use of portable storage devices and enhancement of IT facilities were set out at Annex 1 to the Administration's paper (LC Paper No. CB(1)326/08-09(04)). Where appropriate, international standards such as BS7799 and ISO17799 had been incorporated in the security guidelines for compliance. GCIO and DGCIO(C&O) assured members that the Government would keep in view security challenges

resulting from technological advancement, and would spare no effort to uphold a high standard of information security in keeping with the international standards.

Hong Kong Police

30. Ms Emily LAU noted that a number of recommendations had been made for further improvement following a review of patient data protection by the Hospital Authority's Task Force on Patient Data Security and Privacy as well as PCPD's inspection of the HA's Personal Data System. Ms LAU suggested that an independent third party, preferably the PCPD, should be tasked to review the information security system and practices of the Hong Kong Police Force (HKPF) and make recommendations for improvement.

31. Sharing a similar view, the Deputy Chairman expressed grave concern over the series of data leakages in the HKPF. He doubted whether the successive leakages were due to the top management's low alertness and commitment in creating among staff a culture that protected personal and sensitive data. He asked whether the Office of the Government Chief Information Officer had taken up the matter with the Commissioner of Police (C of P) in person to impress upon him the importance of information security and his responsibility to take remedial action to rectify the situation. He also enquired about the findings of the security risk assessment conducted on the HKPF and whether the level of information security in the HKPF was up to the required standard.

32. In response, GCIO agreed that top management support was vital in fostering a culture that protected personal and sensitive data. He said that the senior management in the HKPF had taken a serious attitude towards the leakages and had adopted rectification measures and risk mitigation safeguards to prevent re-occurrence of such incidents. A number of initiatives as set out in Annex 2 to the Administration's paper (LC Paper No. CB(1)326/08-09(04)), including the setting up of a Force level Working Group to identify the causes of data leakage and address the problem, reviewing information security policies and guidelines, strengthening the control on the use of USB storage devices, the adoption of advanced data protection technologies, as well as training and education programmes had been launched. DGCIO (C&O) said that the HKPF, same as other bureaux/departments, was subject to periodic compliance audit by independent third party companies and was found to have satisfied the required standard which was in line with high international standards. The findings of the report and recommendations for improvement, if any, would be forwarded to the C of P for follow-up. In response to the Deputy Chairman's request, the Administration agreed to provide information on the outcome and findings of the security risk assessment conducted on the security provisions for the staff of HKPF in handling personal or sensitive data, including working outside of the office environment, as well as improvement programmes and follow-up actions to mitigate risk factors identified.

Admin

Measures to prevent data leakage

33. Noting that top management staff from various Bureaux/departments had recently been briefed by a member of the team that reviewed the UK Government's loss of personal data concerning several million UK residents, Ms Emily LAU enquired about the lessons learnt from the review.

34. In reply, DGCIO(C&O) said that the findings of the UK incident revealed problems similar to Hong Kong, such as low level of staff awareness about information security, and the need to step up internal information security management and strengthen relevant security regulations. In this regard, the Administration would accord high priority to promoting staff awareness of security measures and guidelines through education and training, enhancing technical and procedural measures, as well as strengthening management arrangements to ensure compliance.

The way forward

35. The Deputy Chairman requested the Administration to take note of members' concern for follow-up and to update the Panel on the progress of existing and planned security enhancement initiatives on a regular basis, the first one in six months' time.

V. Any other business

36. There being no other business, the meeting ended at 4:00 pm.

Council Business Division 1
Legislative Council Secretariat
8 April 2009