立法會
Legislative Council

LC Paper No. CB(2)963/08-09
(These minutes have been seen by the Administration)

Ref : CB2/PL/SE

Panel on Security

Minutes of meeting
held on Tuesday, 6 January 2009, at 2:30 pm
in Conference Room A of the Legislative Council Building

Members present	:	Hon LAU Kong-wah, JP (Chairman) Hon James TO Kun-sun (Deputy Chairman) Hon Emily LAU Wai-hing, JP Hon Abraham SHEK Lai-him, SBS, JP Hon Audrey EU Yuet-mee, SC, JP Hon Andrew LEUNG Kwan-yuen, SBS, JP Hon LEUNG Kwok-hung Hon CHIM Pui-chung Hon CHAN Hak-kan Hon WONG Kwok-kin, BBS Hon WONG Yuk-man Hon IP Kwok-him, GBS, JP
Members absent	:	Hon Albert HO Chun-yan Dr Hon Margaret NG Hon CHEUNG Man-kwong Dr Hon Philip WONG Yu-hong, GBS Hon WONG Yung-kan, SBS, JP Hon LAU Wong-fat, GBM, GBS, JP Hon Timothy FOK Tsun-ting, GBS, JP
Public Officers attending	:	Item IV Mr W H CHOW Principal Assistant Secretary for Security (D) Mrs Jacqueline KWAN Assistant Director of Immigration (Information Systems)

Mrs Bonnie SMITH
Deputy Privacy Commissioner for Personal Data

Mr Allen TING
Chief Privacy Compliance Officer

Item V

Mrs Jessie TING, JP
Deputy Secretary for Security

Mr David LAU
Principal Assistant Secretary for Security (A)

Mr Luke AU YEUNG Ho-lok, C.M.S.M.
Deputy Commissioner of Customs & Excise

Mr Daniel CHEUNG Chi-kwong
Senior Staff Officer (Information Technology)
Customs and Excise Department

Ms Amy TSE Suk-han
Senior Systems Manager (Information Technology Management Group)
Customs and Excise Department

Item VI

Mr Paul CHENG
Principal Assistant Secretary for Security (B)

Mr YAU Chi-chiu
Assistant Commissioner of Correctional Services (Operations)

Mr William WONG
Electronics & Data Communication Manager
Electrical and Mechanical Services Department

Clerk in attendance : Mr Raymond LAM
Chief Council Secretary (2) 1

Staff in attendance : Mr LEE Yu-sung
Senior Assistant Legal Adviser 1

Mr YICK Wing-kin
Assistant Legal Adviser 8

Miss Josephine SO
Senior Council Secretary (2) 1

Miss Florence WONG
Senior Council Secretary (2) 5

Miss Helen DIN
Legislative Assistant (2) 1

Action

I. Confirmation of minutes of previous meeting
(LC Paper No. CB(2)524/08-09)

The minutes of the special meeting held on 21 October 2008 were confirmed.

II. Information papers issued since the last meeting
(LC Paper Nos. CB(2)473/08-09(01) and CB(2)489/08-09(01))

2. Members noted that the following papers had been issued since the last meeting -

(a) a submission from Hong Kong Women's Coalition on Equal Opportunities on a recent case where a Police officer was accused of raping a young woman inside a Police station; and

(b) a submission from 準來港婦女關注組 on issues relating to immigration control on Mainland pregnant women whose spouses are Hong Kong residents.

3. Ms Emily LAU referred to the submission from Hong Kong Women's Coalition on Equal Opportunities and asked whether follow-up actions would be taken by the Panel. The Chairman said that as agreed at the last meeting, prior to the receipt of the said submission, the Secretariat had written to request the Administration to provide information about the management and security of police stations in view of the media reports on a case in which a police officer was alleged to have raped a young woman inside a police station. Noting that a copy of the submission had been forwarded to the Administration, members agreed that the Administration should be requested to provide a written response to the views and concerns raised in the submission before the special meeting of the Panel scheduled for 21 January 2009. The Chairman said that as the Commissioner of Police (CP) would brief the Panel

Admin

Action

on the crime situation in 2008 on 21 January 2009, members might consider following up the issue with CP at that meeting.

III. Date of next meeting and items for discussion
(LC Paper Nos. CB(2)555/08-09(01) & (02))

Regular meeting in February 2009

4. Members agreed that the following items would be discussed at the next regular meeting to be held on 3 February 2009 and the meeting time would be extended by 30 minutes and advanced to start at 2:00 pm -

(a) Concluding observations of the Committee Against Torture on the second periodic report of the Hong Kong Special Administrative Region under the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment;

(b) Procurement of one mobile X-ray vehicle scanning system by the Customs and Excise Department;

(c) Replacement of radio communications system for the Customs Drug Investigation Bureau of the Customs and Excise Department; and

(d) Delegation of authority for the issuance of Fire Hazard Abatement Notice.

Members agreed that deputations which had provided views to the Committee Against Torture should be invited to give views on item (a).

Regulation of indoor fireworks display

5. Ms Audrey EU expressed concern about the recent fatal nightclub blaze in Thailand, which was reported to have been caused by indoor fireworks display. She suggested that the Administration should be requested to provide information on the regulation of indoor fireworks display, especially those inside entertainment establishments, in Hong Kong and the measures adopted by the Administration to prevent the occurrence of such incidents in Hong Kong.

Admin

IV. Pilot Scheme on Express e-Channel
(LC Paper Nos. CB(2)555/08-09(03) to (05))

6. Principal Assistant Secretary for Security (D) briefed members on the

Action

plan of the Immigration Department (ImmD) to launch the pilot scheme on Express e-Channel in February 2009 at the Lo Wu Control Point (LWCP).

7. With the aid of powerpoint presentation, Assistant Director of Immigration (Information Systems) (AD of Imm) gave members an overview on Express e-Channels.

(*Post-meeting note*: The softcopy of the powerpoint presentation materials was issued to members vide LC Paper No. CB(2)599/08-09(01) on 6 January 2009.)

8. At the invitation of the Chairman, Deputy Privacy Commissioner for Personal Data (DPC) highlighted the views of the Privacy Commissioner for Personal Data (PC) on the implementation of the pilot scheme on Express e-Channel.

9. Responding to Mr IP Kwok-him's enquiries about the enrolment and clearance processes with the use of Express e-Channels, AD of Imm explained that -

(a) ImmD intended to commence the pilot scheme on Express e-Channel in February 2009 at LWCP. As enrolment for using Express e-Channels needed to be done through designated e-Channels, 10 enrolment e-Channels would be installed at LWCP for such purpose;

(b) after enrolment into the scheme, passengers could complete the clearance procedures through one of the 10 Express e-Channels. ImmD would set up overhead display boards and sign-posts to indicate clearly the locations of the enrolment e-Channels and Express e-Channels;

(c) enrolment was a one-off exercise. Passengers already enrolled for using Express e-Channels would not be required to register again even if the service was to be extended to other control points in future; and

(d) ImmD would make available leaflets, posters and videos explaining the enrolment process and the data to be retrieved and stored. Staff of ImmD would be deployed to assist users in enrolling for and using Express e-Channels.

10. Mr IP Kwok-him said that to his knowledge, a small percentage of Hong Kong residents (about 0.7%) could not use their smart identity cards for automated immigration clearance through the e-Channel system due to fingerprint recognition problem. He asked whether the Administration had

Action

estimated the number of people who could not use automated immigration clearance at Express e-Channels, and whether measures would be introduced to reduce failure in fingerprint verification.

11. AD of Imm responded that some people with blurred fingerprints might have difficulty in using e-Channels. It was because the fingerprint scanner used on the spot might not be able to capture a good fingerprint image. In some circumstances, for example, when the weather was dry, the fingerprint identification problem was more distinct. Statistics showed that less than 1% of smart identity card holders had such a problem.

12. Ms Audrey EU said that she had experienced difficulties in using the e-Channels due to fingerprint recognition problem. Noting that some 1% of smart identity card holders were affected, she expressed concern as to whether the Administration would adopt measures to improve the present situation. She asked under what circumstances the Express e-Channel service would delay rather than expedite the clearance process. She also asked about the kind of personal data that would be retrieved and stored in ImmD's back-end servers should a smart identity card holder opt to enrol for using Express e-Channels, and how ImmD would ensure that information newly added to the chip of the Hong Kong smart identity card could be updated to the database kept in the servers. She also asked about the procedures for participants to withdraw from using Express e-Channels.

13. In response, AD of Imm made the following points -

(a) when a passenger inserted his identity card into the card reader at an enrolment e-Channel, the passenger would be invited to give his consent regarding the transfer and storage of his personal data. The relevant data required for performing self-service immigration clearance through Express e-Channels, which were stored in the chip of his Hong Kong smart identity card, included Hong Kong identity card number, name, sex, date of birth, date of registration of the identity card, status of Hong Kong residency and fingerprint templates. On obtaining the passenger's consent, these data would then be transferred via a closed and secure network to ImmD's back-end servers for storage. New information thereafter added to the chip of the passenger's smart identity card, except updated information on limit of stay, would not be required for immigration clearance purpose through the Express e-Channel system;

(b) at an Express e-Channel, the fingerprint captured by the scanner on the spot would be verified against the fingerprint template stored in the back-end servers at LWCP instead of the chip of a smart identity card. Since retrieving information from the back-

Action

end servers was faster, the clearance process involving Express e-Channels would take a shorter time as compared with traditional e-Channels. Express e-Channels would shorten the processing time by about four seconds;

(c) to address the problem associated with fingerprint capturing and matching, ImmD was exploring the feasibility of using optical fingerprint scanners in order to get good fingerprint image. ImmD was in the process of testing these devices. If optical fingerprint scanners were found to be more effective, ImmD would consider wider use, by phases, of these devices in other boundary control points; and

(d) a passenger who had given consent to enrol in the Express e-Channel system might withdraw from the scheme by completing and returning to ImmD a purposely designed form. On receipt of his written notice, ImmD would delete the relevant data stored in the back-end servers.

14. Noting from the paper provided by the Office of the Privacy Commissioner for Personal Data that ImmD had appointed an independent contractor to carry out a security audit on its information technology (IT) system, the Deputy Chairman asked whether the IT Security Report issued by the contractor on 15 September 2006 proved to the satisfaction of PC that ImmD had put in place sufficient measures to protect data privacy in launching the pilot scheme on Express e-Channel. He also asked about the difference in terms of security level between the existing e-Channel system and the Express e-Channel system.

15. DPC and AD of Imm responded that -

(a) the security audit was carried out by an independent contractor. After examination of the said report, PC was of the view that the privacy concerns appeared to have been properly addressed in the system design of the Express e-Channel system;

(b) ImmD had commenced another round of IT security audit in December 2008 to confirm that the security of the system and data as well as access control were in compliance with the Government's security requirements and the personal data protection principles under the Personal Data (Privacy) Ordinance; and

(c) the security level of the new system would be comparable to that of the e-Channel system. The authentication procedures built into the e-Channel system in relation to retrieval of fingerprint

Action

template and identity verification were strict security measures to safeguard the security of data and protect them from unauthorized access or change. Regarding the Express e-Channel system, the back-end servers would be installed at computer rooms purpose-built in compliance with the relevant security requirements. Only authorized officers of the rank of Immigration Officer or above could gain access to the data at designated computer terminals. The new system would keep records of all access to the database for security auditing. Moreover, the computer system of ImmD would have intrusion detection system to prevent hacking and intrusion.

16. Mr LEUNG Kwok-hung asked about the merits of using Express e-Channels. He also asked whether the installation of optical fingerprint scanners in all boundary control points could be advanced to facilitate passengers with blurred fingerprints to undergo self-service immigration clearance. In his view, the procedures for de-registration from the Express e-Channel scheme were too cumbersome and time-consuming. He enquired whether withdrawal could be done at self-service enrolment e-Channels.

17. In response, AD of Imm said that statistics showed that there had been a significant growth in the volume of passenger traffic at LWCP, and about 15 000 passengers were daily users of the e-Channel system. As Express e-Channels could shorten the processing time for immigration clearance by about four seconds for each passenger, the installation of Express e-Channels at boundary control points would help enhance the handling capacity of the control points. As a trial measure to improve the flow of cross-boundary passengers, a small quantity of optical fingerprint scanners had been installed at LWCP. Passengers who persistently had difficulties in using the e-Channels due to fingerprint recognition problem could visit the enrolment office located at LWCP to provide better fingerprint image for future verification purpose at the Express e-Channel. Regarding the procedures for de-registration, AD of Imm said that ImmD would review the experience of the pilot scheme in the second half of 2009. The number of withdrawals would be considered in assessing the suitability of extending Express e-Channels to other control points.

18. Mr CHAN Hak-kan said that many past incidents indicated that the major cause of data leakage was a lack of awareness and understanding among the staff of the security regulations and the risk of compromising personal data. He sought information on the safeguards to be put in place to ensure that data stored in the back-end servers at LWCP were afforded appropriate protection.

19. The Deputy Chairman and Mr LEUNG Kwok-hung shared Mr CHAN Hak-kan's concern about system control and security. Mr LEUNG expressed concern about the rank of the officers authorized to enter the computer rooms.

Action

He held the view that officers should be permitted entry under strict conditions. Steps required to be taken before an officer was permitted entry to the computer room located at the Immigration Headquarters, such as identity verification by means of iris recognition, had to be adopted at LWCP. The Deputy Chairman asked about the chance of information leakage when fingerprint templates captured by the scanners on the spot were stored in the back-end servers at LWCP.

20. AD of Imm responded that the previous case of leakage of confidential information held by ImmD involved an Immigration Officer who had copied some document files which he prepared during work to his personal computer at home and thereafter the leakage of documents containing identifiable personal data on the Internet through Foxy, a peer-to-peer file sharing application. After the incident, all staff members of ImmD were immediately reminded to remove relevant file documents and file sharing applications from their computers at home. To enhance staff awareness, relevant security guidelines and regulations on data protection and the proper handling of personal data were circulated to all immigration staff. AD of Imm stressed that ImmD attached great importance to the protection of personal data privacy. The Express e-Channel system would be subject to strict security measures as specified in paragraph 8 of the Administration's paper. Apart from the use of security token, password and user name, personal particulars would be encrypted before storage in the servers. Furthermore, the servers at LWCP were installed at computer rooms purpose-built in compliance with the relevant security requirements. AD of Imm assured members that there was no question of data leakage from back-end servers. As USB connectivity was not provided in the design of the system, all personal data stored in the servers, including fingerprint templates encoded in strings of binary digits, could not be downloaded to portable electronic storage devices.

21. Mr CHAN Hak-kan pointed out that the traditional immigration counters at most control points were located at the far end of the arrival/ departure halls. He considered that it was very inconvenient to travellers, especially the elderly who might not know how to use the automated passenger clearance system. Mr CHAN suggested that ImmD should consider relocating some traditional counters to the inner part of the arrival/departure halls to facilitate passengers who used traditional counters. AD of Imm noted the suggestion.

22. Ms Emily LAU shared the view that ImmD should adopt appropriate measures to protect the personal data stored in the back-end servers against unauthorized access or disclosure. She asked whether and when the pilot scheme on Express e-Channel would be extended to other boundary control points.

Action

23. AD of Imm responded that ImmD would review the pilot scheme in the second half of 2009. ImmD estimated that some 600 000 frequent travellers, who made cross-boundary journeys to and from LWCP at least once in every two weeks, might find it easier and more convenient to perform self-service immigration clearance through Express e-Channels and hence opt to enrol for the service. If the service was well received by the public, the Administration would consider extending the scheme to other control points. Ms Emily LAU requested that the Administration should provide the Panel with the findings of the review once available.

Admin

24. In reply to Ms Emily LAU's enquiry about the practice in other places, AD of Imm said that some cities and countries, including Shenzhen, the United Kingdom (UK) and the Netherlands, had adopted automated passenger clearance systems similar to Express e-Channels to expedite passenger clearance. While the authentication systems in UK and the Netherlands engaged the use of iris data, the Shenzhen side verified a person's identity by fingerprint authentication. All these cities and countries allowed passengers to use the express automated passenger clearance system on enrolment.

25. Mr LEUNG Kwok-hung was concerned whether ImmD would reduce its frontline manpower following the implementation of Express e-Channels. AD of Imm responded that although the installation of Express e-Channels could help increase the overall passenger throughput at LWCP, the department had no plan to reduce the immigration staff manpower because there was no change to the present manning ratio of the gate-keepers.

V. Implementation of Information System Strategy Projects for the Customs and Excise Department

(LC Paper No. CB(2)555/08-09(06))

26. Deputy Secretary for Security (DS for S) briefed members on the Administration's proposal to implement five Information System Strategy (ISS) projects by the Customs and Excise Department (C&ED), as detailed in the Administration's paper.

27. Ms Emily LAU expressed support for the proposal of C&ED to implement the ISS projects. Referring to some past cases involving leakage of personal data held by government bureaux/departments, Ms LAU expressed grave concern about information security under the new systems. Noting that the ISS projects would assist Customs officers at remote offices/control points in carrying out their daily operations more efficiently, she sought detailed information in this regard.

28. In response, DS for S and Deputy Commissioner of Customs & Excise (DC of C&E) made the following points -

Action

(a) following a number of cases involving leakage of personal data in government departments, the Administration had examined measures to enhance the way in which information security was managed and secured. As all the data leakage incidents involved some form of non-compliance with the information security requirements, additional attention would be paid to enhancing staff awareness and education in order to facilitate their compliance with the information security requirements. Measures taken by government bureaux/departments, including C&ED, included review of methods on processing, storing and protection of personal and classified data; re-circulation of relevant rules and guidelines; and conducting regular IT security risk assessment and audits;

(b) the existing C&ED systems had no centralized management system for security administration. The current manual mode for security administration was inefficient and relatively risk-prone. In future, the new Network and Server Infrastructure would connect the backbone network infrastructure in the new Headquarters with offices at other locations, thus linking up all servers and workstations in C&ED. All C&ED users at remote locations would be provided with high-capacity network connection to support their daily operations. By enabling automatic updating of virus signature and software patches as well as configuration of workstation settings, the system security level of all networked servers and workstations would be enhanced;

(c) the existing C&ED systems did not provide users with access to a single source of corporate data. For example, to perform background checks of trader information for risk assessment and enforcement, users needed to go through different systems with data stored in different formats. Historical operational data were stored in offline media in individual application systems. The data access process was time-consuming and thus adversely affected operational efficiency. It was difficult to perform data analysis in the absence of a single repository for corporate data. The future Central Information Repository System would serve as a central information repository that consolidated all operational data shared among various application systems in C&ED. The new System would not only allow timely access by C&ED staff to operational data to facilitate more efficient decision-making, but also be capable of performing analysis of the data stored in the repository; and

Action

(d) the lack of a centralized and secured information exchange platform entailed extra effort in the exchange of operationally essential data between C&ED's systems and external systems, such as those in other government departments. This was operationally inefficient. The Secured Communications Gateway would enable secure and efficient exchange of operationally essential data between C&ED's computer systems and the systems in other partner government departments. It could also support secure data exchange with overseas customs counterparts.

29. Responding to the Deputy Chairman's enquiry about whether all data would only be kept at one location in future, DS for S explained that C&ED currently operated four data centres, i.e. two production data centres and two disaster recovery data centres, at different locations, which were costly to operate and maintain. The scattered data centres prevented the shared use of manpower, storage devices and system monitoring tools. The Centralized Data Centre project would consolidate the four existing data centres into two new data centres, including one primary data centre and one disaster recovery data centre. While the primary data centre would be installed at the new Customs Headquarters Building in North Point, the disaster recovery data centre would be located at C&ED's office in Harbour Building, Central. A backbone network infrastructure would be installed in the new Headquarters to support 24-hour operations of C&ED systems.

30. Noting that the new Secured Communications Gateway would provide C&ED with more efficient interfaces with the systems of other government departments and support information exchange between C&ED and its overseas customs counterparts, the Deputy Chairman asked about the frequency and merits of such exchange.

31. In response, DS for S and DC of C&E said that -

(a) over the decades, C&ED had developed its IT infrastructure and computer systems at different stages on a project-by-project basis without coordinated planning. As a result, there were various small-scale computer systems dedicated to serve specific user groups at different locations with limited sharing capacity. The existing C&ED systems did not provide users with access to a single source of corporate data as explained earlier. As C&ED's existing fragmented IT infrastructure limited the scope for enhancing its performance, there was a need to standardize the IT systems in C&ED;

(b) on customs clearance at control points, Customs officers often needed to cross-check information obtained from other sources. For example, for cargo clearance through the Land Boundary

Action

System and the Automatic Vehicle Recognition System, the licence numbers of vehicles and particulars of drivers stored in the computer systems of the Transport Department (TD) had to be regularly updated to C&ED's system, so as to facilitate the flow of goods and vehicles. The new Secured Communications Gateway was capable of supporting secure information exchange between C&ED and TD; and

(c) although information exchange with overseas customs counterparts was not frequent, the proposed Secured Communications Gateway would provide a secure platform for efficient exchange of operationally essential data with other external parties, if so required. This would enhance C&ED's capability to detect and combat smuggling activities and transnational crimes.

32. The Chairman concluded that the Panel did not object to the submission of the proposal to the Finance Committee for funding approval.

VI. Replacement of the radio communication system of the Correctional Services Department

(LC Paper No. CB(2)555/08-09(07))

33. Members noted the Administration's proposal to replace the existing analogue radio communications system of the Correctional Services Department (CSD) with a new digital system, as detailed in the Administration's paper.

34. The Deputy Chairman said that he supported the proposal to replace CSD's existing analogue radio communications system with a new digital one. Noting the high investment cost of the new system and the normal serviceable life of a radio communications system being 10 to 12 years, he enquired about the expected serviceable life of the new system, and whether there were ways to extend the serviceable life of the new system to enhance its cost-effectiveness.

35. Principal Assistant Secretary for Security (B) (PAS(S)B) and Electronics & Data Communication Manager, Electrical and Mechanical Services Department responded that the existing radio communications system of CSD comprised an Ultra High Frequency (UHF) system and a Very High Frequency (VHF) system. The UHF system served the communication needs of five penal institutions, while the remaining 19 institutions were covered by the VHF system. The two systems had been in use since 1992 and 1998 respectively, and they were approaching the end of their serviceable lives because the analogue technology was becoming obsolete. Moreover, the

Action

systems could not be upgraded to cater for the future operational needs of CSD. It was also increasingly difficult to find spare parts for servicing the obsolete system. The maintenance cost of the system was expected to be high when more and more components become obsolete and had to be specially ordered from the supplier. PAS(S)B advised that the proposed system would bring about the following benefits -

(a) the infrastructure of the proposed system would be built on open technological standards, which allowed the system to be further enhanced and developed in future to meet the changing operational needs of CSD;

(b) the proposed system would offer improved voice quality and better protection against interference and interception;

(c) the proposed system would cover all 24 penal institutions under CSD and enable more efficient communications among institutions; and

(d) the digital technology to be employed in the proposed system was capable of reducing the impact of the shielding effect arising from strong building structure and improving indoor radio communication.

36. PAS(S)B said that in finalizing the design of the new system, suitable room for expansion would be reserved so that the capacity of the system could be enhanced in the light of the changing needs of CSD. As the digital technology would operate on open platform, CSD would have wider choice in case of upgrades or replacement of the system in future. This would help extend the serviceable life of the new system and its cost effectiveness.

37. Responding to the Deputy Chairman's concern about the performance of the existing analogue radio communications system, Assistant Commissioner of Correctional Services (Operations) advised that CSD had alternative communication fallback mode which could support the daily operations of penal institutions and ensure a reliable and secured means of communication among officers on site. He pointed out that most CSD officers on site were required to take up patrol and escort duties, and the use of portable radio handsets was their sole means of communication. CSD would consider acquiring additional radio transceivers to improve the radio coverage before the implementation of the proposed system by 2012.

38. Mr CHAN Hak-kan shared the view of the Deputy Chairman that the Administration should endeavour to extend the serviceable life of CSD's proposed radio communications system, since the new system involved an investment of $101 million. He enquired about the implementation plan, and

Action

the security and technology standards of the proposed system as compared with the one currently in use by the Hong Kong Police Force or the Fire Services Department (FSD).

39. PAS(S)B referred to Annex C of the Administration's paper and advised that the Administration planned to implement the project in phases. The proposed system would cover all 24 penal institutions under CSD. The system would be installed and commissioned by phases and it would be fully commissioned in December 2012. As regards the security and technology standards of the proposed system, PAS(S)B advised that CSD was working in collaboration with the Electrical and Mechanical Services Department to draw up specification of security and technology standards which could meet the operational requirements of CSD. The proposed radio communications system would adopt the Terrestial Trunked Radio technology similar to that currently adopted by the Police and FSD. As different departments had different operational needs, the security and technological requirements of the three systems were not directly comparable.

40. The Deputy Chairman held the view that CSD's proposed radio communications system might not necessarily require the same degree of security and technology standards as that of the Police or FSD.

41. The meeting ended at 4:30 pm.

Council Business Division 2
Legislative Council Secretariat
27 February 2009