立法會
Legislative Council

Ref : CB2/PL/SE

Panel on Security

Minutes of meeting
held on Tuesday, 6 January 2015, at 2:30 pm
in Conference Room 3 of the Legislative Council Complex

Members present	:	Hon IP Kwok-him, GBS, JP (Chairman)
		Hon NG Leung-sing, SBS, JP (Deputy Chairman)
		Hon James TO Kun-sun
		Hon CHAN Kam-lam, SBS, JP
		Hon Emily LAU Wai-hing, JP
		Dr Hon LAM Tai-fai, SBS, JP
		Hon CHAN Kin-por, BBS, JP
		Hon WONG Kwok-kin, SBS
		Hon Paul TSE Wai-chun, JP
		Hon WONG Yuk-man
		Hon Claudia MO
		Hon Frankie YICK Chi-ming
		Hon YIU Si-wing
		Hon MA Fung-kwok, SBS, JP
		Hon Charles Peter MOK, JP
		Dr Hon Kenneth CHAN Ka-lok
		Hon LEUNG Che-cheung, BBS, MH, JP
		Hon Kenneth LEUNG
		Hon KWOK Wai-keung
		Hon Dennis KWOK
		Hon Christopher CHEUNG Wah-fung, SBS, JP
		Dr Hon Fernando CHEUNG Chiu-hung
		Dr Hon Elizabeth QUAT, JP
		Dr Hon CHIANG Lai-wan, JP
		Hon CHUNG Kwok-pan
		Hon Christopher CHUNG Shu-kun, BBS, MH, JP

Member attending	:	Hon Albert CHAN Wai-yip

Members absent	:	Hon Cyd HO Sau-lan, JP Dr Hon Priscilla LEUNG Mei-fun, SBS, JP Hon Alan LEONG Kah-kit, SC Hon LEUNG Kwok-hung Hon Michael TIEN Puk-sun, BBS, JP Hon CHAN Chi-chuen

Public Officers attending	:	<u>Item IV</u> Mr John LEE Ka-chiu, PDSM, PMSM, JP Under Secretary for Security Mr Billy WOO Tak-ying Principal Assistant Secretary for Security D Mr Corrado CHOW, IDSM Assistant Director (Information Systems) Immigration Department Mr David CHIU Wai-kai, IDSM Assistant Director (Personal Documentation) Immigration Department Miss Caroline FAN Mei-hing Chief Systems Manager (Technology Services) Immigration Department

Clerk in attendance	:	Miss Betty MA Chief Council Secretary (2) 1

Staff in attendance	:	Mr Bonny LOO Assistant Legal Adviser 3 Mr Raymond LAM Senior Council Secretary (2) 7 Miss Lulu YEUNG Clerical Assistant (2) 1

Action

I. Confirmation of minutes of previous meeting
(LC Paper No. CB(2)532/14-15)

The minutes of the meeting held on 2 December 2014 were confirmed.

II. Information papers issued since the last meeting
(LC Paper Nos. CB(2)418/14-15(01), CB(2)419/14-15(01), CB(2)511/14-15(01), CB(2)529/14-15(01) and CB(2)563/14-15(01))

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

(a) letter dated 3 December 2014 from Ms Claudia MO regarding use of explosives by members of the public to kill animals and the Administration's mechanism for handling items suspected to be explosives;

(b) Administration's interim response and further response to issues raised in the letter dated 3 December 2014 from Ms Claudia MO;

(c) letter dated 4 December 2014 from Prof Joseph LEE regarding the Police's use of force against healthcare personnel in recent public assemblies; and

(d) letter dated 2 January 2015 from Ms Claudia MO regarding the Police's application for orders for care and protection of children and juveniles.

3. Members agreed that the Administration be requested to provide a response to the issues raised in the letter dated 2 January 2015 from Ms Claudia MO.

III. Date of next meeting and items for discussion
(LC Paper Nos. CB(2)534/14-15(01) and (02))

Regular meeting in February 2015

4. Members agreed that the following items would be discussed at the next regular meeting on 3 February 2015 at 2:30 pm -

(a) Briefing by the Secretary for Security on the Chief Executive's 2015 Policy Address; and

(b) Briefing by the Commissioner, Independent Commission Against Corruption on the Chief Executive's 2015 Policy Address.

5. The Chairman informed members that he had received a joint letter from Mr James TO, Ms Cyd HO and Mr Kenneth LEUNG proposing the appointment of a subcommittee under the Panel to review the Police's guidelines and procedures on the use of force as well as facilitating media reporting work at public assemblies. The Chairman said that the proposal would be included in the agenda for the next regular meeting on 3 February 2015.

Special meeting on 27 January 2015

6. The Chairman reminded members that a special meeting would be held on 27 January 2015 from 2:00 pm to 4:00 pm to receive a briefing by the Commissioner of Police on the crime situation in 2014.

IV. The next generation Smart Identity Card System
(LC Paper Nos. CB(2)534/14-15(03) and (04))

7. Under Secretary for Security ("US for S") briefed Members on the Administration's proposal to implement the Next Generation Smart Identity Card System ("SMARTICS-2") and the introduction of the next generation smart identity ("ID") card. With the aid of powerpoint presentation, Assistant Director of Immigration (Information Systems) ("AD of Imm (IS)") briefed Members on the salient features of SMARTICS-2 and the proposed next generation smart ID card as well as the proposed ID card replacement exercise.

8. Members noted a background brief entitled "Smart identity card" prepared by the Legislative Council Secretariat.

Security of the proposed new smart ID cards under wireless technology

9. Mr Dennis KWOK asked whether Radio Frequency Identification ("RFID") technology would be deployed for the proposed new smart ID cards. He expressed concern that as RFID technology would enable the

reading of information stored inside smart cards within a certain distance, someone with a suitable device might be able to read information stored in the chip of a new smart ID card from a distance without being noticed by the cardholder. Such act was in contravention of the Basic Law and the Immigration Ordinance ("IO") (Cap. 115). Ms Claudia MO expressed concern that if such wireless technology was adopted, someone possessing the necessary decryption keys might be able to read information stored in a new smart ID card without being noticed. She asked whether the Administration could assure that such unauthorised access to information in a smart ID card would not happen.

10.   US for S responded that the proposed new smart ID cards would adopt a bi-level encryption mechanism and the question of someone, without being authorised, reading information stored inside a new smart ID card would not be allowed. To enable access to information in a new smart ID card, it would be necessary to physically place the smart ID card onto an optical card reader ("OCR"), which would capture certain unique card face data to start the communication. Such unique card face data would be scanned by the card reader and an access key would be generated. Mutual authentication between the new smart ID card and reader would then follow. Only after the authentication was successful would the encrypted communication channel be established between the smart ID card and the reader. To access data stored in the chip of the smart ID card, further mutual authentication between the chip and the reader was required. The smart ID card had to be placed firmly onto OCR to read the card face data. For the card reader to retrieve data from the chip, the distance between it and the card had to be within 2 cm. He said that the scope of information obtainable from a new smart ID card with OCR reader would be kept to a minimum. The proposed technology was already widely used in many European countries, including Germany and Finland. Such technology had also been adopted for the Hong Kong Special Administrative Region passport. AD of Imm (IS) added that the existing system employed Public Key Infrastructure ("PKI") encryption, while the proposed system would employ both Basic Access Control ("BAC") mechanism and PKI encryption technology.

11.   Mr Charles MOK said that although the explanation given by the Administration was acceptable from a technical point of view, there were concerns in overseas countries about the security level of encryption codes of smart ID cards and passports, such as ease of identifying the pattern of encryption codes. He considered that the Administration should provide more detailed information on the security and technical aspects of the proposed new system and smart ID card to address public

concerns about the possibility of information inside a new smart ID card being read by another person at a distance without being noticed by the cardholder. It should provide a detailed comparison between the security features of SMARTICS-2 and the systems currently used in overseas countries. The Administration should also invite some academics and experts in RFID to provide independent views on the security of SMARTICS-2 and the possibility of remote access to information in the smart ID card.

12. Referring to footnote 4 on page 5 of the Administration's paper, Mr Charles MOK asked whether the Administration had not arrived at a decision on whether to introduce access control mechanism through optical means before enabling wireless communication of the chip. AD of Imm (IS) responded that consideration was also being given to the use of other access control mechanisms with higher security level, such as Password Authenticated Connection Establishment or Supplemental Access Control.

13. Mr Albert CHAN considered that financial provisions for the proposed new smart ID cards and related system should be reserved for other initiatives, such as the provision of dental treatment to the elderly. He expressed concern that the new smart ID cards might be open to abuse. US for S responded that there was no question of abuse of the proposed new smart ID cards and related system by law enforcement officers, who were required to act in accordance with the law.

14. Mr WONG Yuk-man queried why there was a need to replace smart ID cards seven years after completion of the last card replacement exercise in 2007. He also queried why smart ID cards and the system concerned had to be replaced at the same time. He considered that the Administration should provide detailed information on the security of the proposed new smart ID cards and related system to address concerns of the public about remote access to information stored in a smart ID card. Referring to paragraph 15 of the Administration's paper, he said that the Administration should provide the Panel with the findings, if any, of Privacy Impact Assessments conducted on the proposed new smart ID cards and related system.

15. Noting that some Members were concerned about the use of RFID technology in the proposed new smart ID card, Dr Elizabeth QUAT asked why there was a need to employ such technology. Mr Christopher CHEUNG asked whether a contactless smart ID card would have a lower failure rate in comparison with a "contact type" smart ID card.

Action

16.   AD of Imm (IS) responded that it was the international trend to use contactless smart ID cards, which were more durable and had a lower failure rate than "contact type" smart ID cards. The data transmission speed of a contactless smart ID card would be much faster than that of a "contact type" smart ID card. The chip of a contactless smart ID card would be more durable, as it would be embedded in a smart ID card and thus not exposed to damage by the environment. He said that the smart ID card system currently used in Germany was employing the same technology as that proposed by the Administration.

17.   Noting that there was an international trend towards the use of wireless technology for smart cards, Mr MA Fung-kwok asked why "contact type" smart card technology would still be employed for the new smart ID cards. AD of Imm (IS) responded that the existing smart ID card also served as a library card for those cardholders who had chosen such an application and "contact type" smart card technology was still being used by the Leisure and Cultural Services Department.

18.   Mr MA Fung-kwok sought information on the possibility of access to information in the chip of a smart ID card by parties other than the Government. Dr Elizabeth QUAT asked whether cases of remote access to information stored in the chip of a smart ID card had so far been identified in any country. AD of Imm (IS) responded that although there were reports about the use of RFID technology for provision of remote access to information, there had not been any reports about access to information stored inside the chip of a smart card without the knowledge of the cardholder. US for S stressed that under the proposed system, a smart ID card had to be placed within a distance of 2 cm from an OCR before the card face data could be captured by the OCR.

19.   Dr CHIANG Lai-wan asked whether a new smart ID card could be used for tracking the cardholder. AD of Imm (IS) replied that a smart ID card could not be used for tracking, as there was no power supply inside a smart ID card and the retrieval of data from the chip of a smart ID card required a distance of 2 cm or less between the smart ID card and OCR.

20.   Mr Paul TSE asked whether it would be much easier to compromise a person's personal information with a mobile phone than smart ID card. US for S said that the security and privacy protection of the proposed ID card system was far higher and stronger than mobile phones.

Action

21.   <u>Ms Emily LAU</u> said that she had requested the Administration on the previous day to provide more detailed information on the security and privacy aspects of the proposed new smart ID cards and related system to address concerns regarding the possibility of remote access to information stored inside a new smart ID card. She queried why the Administration had not provided the information requested. She said that the Panel should consider holding a meeting to receive the views of the public on the Administration's proposal.

Admin

22.   <u>US for S</u> responded that extra information had been included in the powerpoint presentation as a result of the Administration's meeting with Ms Emily LAU on the pervious day. As regards information on the technological side, it was considered that direct explanation by the responsible officers at the Panel would be more helpful. In view of members' concern despite the explanation, the Administration would provide supplementary information on the security and privacy aspects of the proposed system as well as measures to prevent remote access to information stored inside a new smart ID card.

23.   <u>Mr Christopher CHEUNG</u> expressed support for the Administration's proposed system, which would shorten immigration clearance time. He asked whether the proposed new system would be encrypted to prevent unauthorised access to information stored in the chip of a smart ID card. <u>Dr CHANG Lai-wan</u> sought information on the major differences in terms of data security between the existing system and the proposed SMARTICS-2.

24.   <u>AD of Imm (IS)</u> explained that while the existing system employed PKI encryption technology only, the proposed new system would employ BAC mechanism on top of PKI encryption technology and data transmission would be made through dedicated encrypted communication channels. He pointed out that PKI encryption technology had been employed in the existing smart ID card system for about 11 years and there had not been any case of leakage of information stored in the chip of a smart ID card.

25.   <u>Mr James TO</u> said that the Administration should consider arranging a demonstration for members to better understand the operation and security features of SMARTICS-2 as well as new smart ID cards. He expressed concern about the possibility of suppliers of new smart ID cards providing decryption keys to personnel of Mainland authorities or other countries, thus enabling such personnel to access information stored

Action

inside the chips of new smart ID cards. As there were public concerns about unauthorised access to information stored inside the chip of a smart ID card and some people might consider it unnecessary to reduce the clearance time at e-Channels from 12 seconds to 8 seconds, he asked whether the Administration would abandon its plan to employ wireless transmission technology in the proposed new smart ID cards and related system.

26. Dr Fernando CHEUNG said that ID cards were not issued to residents of the United States of America. The United Kingdom had also abolished requirements for its residents to produce ID cards when requested by law enforcement officers. He expressed concern that although the Administration had stressed that remote access to the chip of a smart ID card was not possible, there might be future technological development enabling unauthorised remote access to information stored inside the chip of a smart ID card. Referring to paragraphs 6 and 7 of the Administration's paper, he said that the Administration should provide members with the findings of the consultancy study and feasibility study concerned.

27. US for S reiterated that it was the international trend to use contactless smart ID cards and similar technology was already in use in many European countries. He said that the Administration would provide members with supplementary information on the security and privacy protection features of the proposed new smart ID cards and related system. He reiterated that under the proposed system, a smart ID card had to be placed within a distance of 2 cm from an OCR before the card face data could be captured and any communication with or reading of the card could begin.

28. Dr LAM Tai-fai said that as smart ID cards would not last for ever, there was a need for replacement of existing smart ID cards and he could not see any grounds for objection. He said that citizens who abided by the law were not suspicious about the need for smart ID card replacement.

29. Mr Kenneth LEUNG requested the Administration to provide information on the countries belonging to the Organization for Economic Cooperation and Development ("OECD") which had issued ID cards to residents as well as OECD countries which required residents to produce ID card or other proof of identity when required by police officers or relevant law enforcement officers. US for S agreed to provide a written response.

Admin

Scope of information stored in the chip of a smart ID card

30.　Mr Kenneth LEUNG sought information on the scope of information stored in the chip of a smart ID card. US for S responded that information stored in the chip of an existing smart ID card was provided for in the Registration of Persons Ordinance (Cap. 177) ("ROPO"). Information such as name, Chinese Commercial Code of the Chinese name, sex, photograph, fingerprint templates, right of abode status as well as the condition of stay, if any, in the case of a non-permanent resident, was stored on the smart ID card.

31.　Mr Kenneth LEUNG asked whether the Administration could assure the storage of no information other than that set out in ROPO in the chip of a smart ID card. Mr Christopher CHUNG asked whether licences issued by other government departments, such as driving licence, could be incorporated into the new smart ID card.

32.　US for S responded that the storage of information other than that provided in ROPO would require the consent of the cardholder concerned. In this connection, the Office of the Government Chief Information Officer ("OGCIO") was conducting a separate technical study to review other possible uses of smart ID cards.

33.　Mr Kenneth LEUNG asked whether the Administration had reviewed the requirements in section 17C of IO for residents to produce ID card or other proof of identity when required by police officers or relevant public officers. US for S responded that there was a need for the requirements in section 17C of IO for maintaining law and order as well as the security of Hong Kong.

Serviceable life span of smart ID cards

34.　Mr WONG Kwok-kin considered that the replacement of smart ID cards at around 10-year intervals might create inconvenience to residents. He sought information on the estimated life span of the proposed new smart ID cards. He expressed concern about the worst situation which might arise, if the existing smart ID cards and related system were not replaced.

35.   <u>Mr YIU Si-wing</u> also expressed concern about the serviceable lifespan of the proposed new smart ID cards. He considered that the Administration should require the supplier to provide new smart cards made of more durable polycarbonate materials. <u>Mr Christopher CHUNG</u> expressed concern about the performance of the new smart ID cards under extreme temperatures.

36.   <u>US for S</u> responded that the serviceable life span of the existing smart ID card had been guaranteed by the manufacturer for 10 years under normal usage. Independent laboratories had confirmed this and had not found any proof to guarantee its use beyond 10 years. The Administration had secured extension of the existing system maintenance agreements to the end of 2018, by which time the first batch of smart ID cards issued in 2003 would have been in use for about 15 years. He said that there was currently an average of about 100 malfunction incidents of the existing computer system per year. Breakdowns of the image storage system, for example, had increased from five cases per year to 32 cases per year in the past five years. With the ageing of existing smart ID cards, the possibility of massive card failure would increase. It would be irresponsible to continue using the existing smart ID cards and related system far beyond their serviceable lifespan, as a massive breakdown and malfunction of existing smart ID cards might result in confusion in immigration clearance and pose threat to the security of Hong Kong.

37.   <u>Mr KWOK Wai-keung</u> considered that the replacement of existing smart ID cards should be based on the life span of existing smart ID cards and the Administration should set out its requirements on the life span of new smart ID cards in the tender invitation. <u>US for S</u> responded that the Administration also hoped that the system would have a longer life span and would consider this in the tender exercise.

<u>Forgery of smart ID cards and reliability of existing smart ID cards</u>

38.   <u>Mr LEUNG Che-cheung</u> expressed concern about the number of forged smart ID cards seized in a year. <u>Dr LAM Tai-fai</u> also expressed concern about the number of forged smart ID cards identified so far by the Administration. <u>US for S</u> responded that 3 258 forged ID cards had so far been seized, representing 0.028% of the total number of smart ID cards issued. The quantity of forged smart ID cards seized had been small and the technology employed in the forged cards was not advanced.

39.   Noting that around 11 million smart ID cards had so far been issued but the population of Hong Kong was less than eight million, Mr LEUNG Che-cheung expressed concern about whether there was a large number of smart ID cards requiring replacement because of card failure. US for S responded that about 63 000 smart ID cards had so far been replaced for problems associated with chips, representing about 0.5% of the total number of smart ID cards issued. In 2013, around 25 000 smart ID cards had been replaced mainly for damage of polycarbonate materials of the cards.

40.   Assistant Director of Immigration (Personal Documentation) ("AD of Imm (PD)") explained that a child at the age of 11 would be issued a smart ID card, which would be replaced by an adult ID card at the age of 18. Persons granted with employment visas, such as foreign domestic helpers, would also be issued with smart ID cards. The smart ID cards of new arrivals from the Mainland with One-way Permits would also be replaced when they became permanent residents after meeting the seven-year residence requirement. The total number of smart ID cards issued was thus more than the population of Hong Kong.

New functions to be incorporated in the new smart ID card

41.   Mr CHAN Kam-lam sought information on the new applications, such as electronic purse, which might be incorporated into the proposed new smart ID cards.

42.   US for S responded that information stored in the chip of the new smart ID card, regulated by ROPO, would mainly fall into two types, including that for immigration-related applications for verification of the cardholder's identity and that for other applications which required the consent of the cardholder. OGCIO was conducting a separate technical study to review what applications might be included into the second type. The overriding principle was that it would not compromise the security and privacy protection of the new ID card which was principally used for verification of identity for ROPO purpose.

Contingency measures to cope with a possible large-scale failure of the existing smart ID cards

43.   Noting that the existing smart ID card system had reached the end of its serviceable life span, Mr Christopher CHEUNG expressed concern about whether the Administration had any contingency plan in place to cope with a possible large-scale failure of existing smart ID cards, thus

requiring the replacement of a large number of smart ID cards within a short time. His concern was shared by Mr YIU Si-wing, who pointed out that the existing smart ID cards would have been in use for about 18 years when the last batch of ID cards was replaced in 2022.

44.	AD of Imm (PD) responded that in the event of a large scale smart ID card failure, the required card replacement service would be provided by the existing Registration of Persons ("ROP") Offices. Where necessary, the opening hours of ROP Offices would be extended and additional resources would be sought for the necessary increase in manpower.

Memory size of the chip of a smart ID card

45.	Mr MA Fung-kwok asked why the memory size of the chip of a new smart ID card was proposed to be 80 KB, given that the memory size of memory cards available on the market had far exceeded 80 KB. AD of Imm (IS) responded that the chip of a smart ID card differed from a common memory card in that the former incorporated a microprocessor. A memory size of 80 KB was proposed for the new smart ID card because of the memory size needed and cost considerations. Depending on the technological development in respect of chips in the coming years, the Administration would not rule out the adoption of a larger memory size for the chips of new smart ID card.

(As the Chairman had to attend some urgent business, the Deputy Chairman took over the chair at this juncture.)

Issues relating to the ID card replacement period

46.	Dr LAM Tai-fai asked why a period of four years would be required for the replacement of smart ID cards. AD of Imm (IS) responded that the four-year card replacement period was estimated having regard to the experience in the last ID card replacement exercise which commenced in 2003.

47.	Mr Christopher CHUNG considered that the operation hours of card replacement centres should be extended and more replacement centres should be set up. Consideration should be given to allowing cardholders to complete application forms on the web to shorten waiting time at card replacement centres. AD of Imm (IS) responded that while the card replacement period could be shortened by setting up additional card replacement centres, there would be difficulties in identifying

suitable sites for setting up such additional card replacement centres. AD of Imm (PD) added that in the last ID card replacement exercise which commenced in 2003, nine card replacement centres were in operation from 8:00 am to 10:00 pm on a daily basis. Difficulties were encountered at that time in the identification of suitable sites for setting up card replacement centres.

48. Mr Christopher CHUNG asked whether the elderly and persons with disabilities would be exempted from the requirement of attending card replacement centres in person for smart ID card replacement. AD of Imm (PD) responded that there were legal provisions in ROPO to exempt such persons from the requirement of attending the replacement centres in person for card replacement.

Other issues

49. Dr LAM Tai-fai asked whether existing smart ID card readers at immigration control points could cope with the use of existing and new smart ID cards in parallel during the four-year card replacement period. AD of Imm (IS) responded that there were plans to increase the number of e-Channels at various immigration control points. It was expected that about 600 multi-purpose e-Channels capable of reading old and new smart-ID cards would be in use in 2016.

50. Mr KWOK Wai-keung asked how the Administration would dispose of old smart ID cards collected in the card replacement exercise. AD of Imm (IS) responded that the old smart cards would be chopped into small pieces by the Immigration Department ("ImmD") and collected by recycling service providers.

51. Dr CHIANG Lai-wan asked whether the proposed new system and smart cards could be procured from suppliers based in Hong Kong instead of overseas suppliers. AD of Imm (IS) responded that the proposed new system and smart ID cards would be procured under the government's tendering process without restrictions on the place of manufacture.

52. Mr CHAN Kin-por expressed support for the Administration's proposal to replace smart ID cards, which had been in use for about 10 years. He asked whether capacity would be reserved in the new smart ID card for future upgrade. US for S responded that the suppliers would be required to employ the latest technology. He would ask ImmD to consider Mr CHAN's suggestion in designing the new system.

53.   Mr Paul TSE asked whether the Administration had explored the possibility of employing other biometric authentication technologies, such as facial recognition technology, in the verification of a person's identity. US for S responded that the Administration favoured the use of fingerprint authentication technology, which had an accuracy rate of about 99.4%, as well as facial recognition technology, which had an accuracy rate of about 99.7%, in the verification of a person's identity. He said that facial recognition technology would be employed, for example, in the verification of the identity of a visitor leaving Hong Kong. Both methods were reliable and well accepted by the people of Hong Kong. The Administration would, however, continue to keep track of the latest developments in biometric authentication technologies.

Way forward

54.   The Deputy Chairman sought members' view on whether they supported in principle the Administration's submission of its proposal to the Finance Committee ("FC"). Ms Emily LAU and Dr Fernando CHEUNG considered that before the Administration submitted its proposal to FC, the supplementary information to be provided by the Administration should first be discussed by the Panel.

> (*Post-meeting note*: The supplementary information provided by the Administration was subsequently scheduled for discussion under the item "Matters arising" at the meeting on 3 February 2015 with the concurrence of the Chairman.)

V.   Latest situation of the operation of control points
   (LC Paper Nos. CB(2)534/14-15(05) and (06))

55.   Owing to time constraint, members agreed that the item would be deferred to a future meeting.

VI.   Provision of a Barge Operating Platform for the Marine Region of the Hong Kong Police Force
   (LC Paper No. CB(2)534/14-15(07))

56.   Owing to time constraint, members agreed that the item would be deferred to a future meeting.

(*Post-meeting note*: With the concurrence of the Chairman, the item was subsequently scheduled for discussion at the meeting on 3 February 2015.)

57.   There being no other business, the meeting ended at 4:30 pm.

Council Business Division 2
Legislative Council Secretariat
2 February 2015