For information
on 11 October 2002

Bills Committee of the Legislative Council
Registration of Persons (Amendment) Bill 2001

Comments by Hong Kong Computer Society	**Administration's Response**
1. Clause 7 – may need to make provision for digitally/ electronically transfer of data (paragraph 3a)	- Clause 7 (the new section 10) places restriction against disclosure or transfer of ROP data. What the new section prohibits is the act of disclosing, i.e. making known ROP data to third parties, and the prohibition is capable of covering disclosure or transfer by whatever means.
2. Regulation 12(1A)– may need to include unlawful or unauthorised retrieval of data stored in a chip (paragraph 3b)	- We have already included a new Section 11 to the ROP Ordinance so that any person who, without lawful authority or reasonable excuse, gains access to, stores, uses or disclose any particulars furnished to a registration officer shall be guilty of an offence under the ROP Ordinance. These particulars include data in the chip.
3. Clause 23: Schedule 2, item 2 regulation 12(1A) – may need to include alteration or manipulation of data stored. (paragraph 3c)	- The description of offence under Column 3 of Schedule 2 to the Immigration Service Ordinance is to give a general description of the enactment mentioned in Column 2 of the same Schedule. Details of the enactment should be read from the relevant underlying legislation (i.e. regulation 12(1A) of the ROP Regulations in this particular

Comments by Hong Kong Computer Society	Administration's Response
	case). - The new Regulation 12(1A) of the ROP Regulations will make it an offence for any person who, without lawful authority, stores, adds to, erases, cancels or alters any data stored in a chip or renders a chip ineffective.
4. Proper segregation of systems, data and applications, definition of ownership, introduction of appropriate access control, audit trail, checking by backend systems, partitioning of chip, should be implemented. Rigorous assessments should also be conducted in order to address the concerns. (paragraph 4)	- Under the Smart Identity Card System (SMARTICS), data protection measures (both technical and management) have been incorporated to enforce segregation of systems, data and applications from each other so that immigration data on a card will be protected from other applications on the card and vice versa. The system design has been reviewed by an independent data privacy expert and confirmed acceptable.

Security Bureau
10 October 2002