GCIO's opening remarks at ITB panel special meeting on 30 May 2008

1. Mr Chairman, on behalf of the whole Government, let me start by apologizing to everyone whose personal data has been compromised in the recent incidents. We sincerely regret any anxiety and annoyance that have been caused.

2. My Office and the Hospital Authority have each submitted a paper for the panel's consideration. It might be convenient for the panel if I briefly set out the background to all the incidents and the measures that the Government and the HA are taking.

3. In the past two months, there have been reports of 12 cases of lost or stolen portable electronic storage devices, such as USB drives, which held personal data. There have also been two cases of personal data being exposed on the Internet as a result of software installed on staff's home computers. Ten of the lost device cases occurred in the Hospital Authority, one in the Health Department and one in the Civil Service Bureau. The cases of data being exposed on the Internet occurred in the Immigration Department and the Police. Investigations to date have found no compromise of any Departmental core systems or communications networks.

4. I also need to inform the Panel that yesterday afternoon an officer in the Food and Environmental Hygiene Department inadvertently sent an email to a complainant with an attachment that contained sick leave records for 170 FEHD staff.

5. In all cases except that of the Immigration Department, all the people whose personal data was compromised are being informed and advised on any extra care they should take to guard against possible misuse of their data. In the case of the Immigration Department, most of the personal data related to visitors for whom they have no contact information. Reports have been made to the Privacy Commissioner in

respect of all these incidents, and the cases of suspected theft have been reported to the Police.

6. Each of the Bureaux and Departments concerned has taken steps to reduce the risk of further incidents. This has generally involved tightening security procedures, reminding staff of the security requirements and making available software and hardware that staff can use to work more securely.

7. The Government takes information security very seriously and is determined that the lessons learned from these incidents should be applied across all Bureaux and Departments.

8. Human factors have played a significant role in all these incidents. There has been a lack of awareness of the security regulations, a lack of knowledge of how to comply and a lack of understanding of the risks of compromising personal data. These factors have led to unencrypted personal data being stored on portable storage devices and on home PCs which have turned out to have malicious software installed.

9. I shall briefly describe the measures we are taking to address the human and management issues.

10. The Government has tightened the procedures relating to the use of portable storage devices and has reminded all civil servants of these procedures. We are also asking all B/Ds to review the way they manage the risk posed by unauthorised working at home – both by reducing the temptation to work at home without proper authority and by making sure that anyone authorised to work at home is provided with a secure way of doing so. OGCIO will work with Departmental IT Security Officers to support them in these reviews.

11. OGCIO together with Security Bureau and the Civil Service Bureau will also plan a communications programme for Government staff with the aim of building and sustaining awareness of security issues and a culture of protecting personal and classified data.

12. We also plan to enhance staff training. As a first step, we have included a briefing on information security in induction courses for newly-recruited EOs.

13. We intend to strengthen the management arrangements which assure compliance with the security policy and provide guidance to B/Ds, public bodies and NGOs. We will be reviewing the policies and regulations themselves, the content of security audits, and the roles and responsibilities for assuring information security throughout the public sector.

14. Finally, B/Ds will be reviewing their own security practices in the light of these measures. As well as the B/Ds involved in recent incidents, some other B/Ds have already embarked on reviews and have enhanced staff communications. For instance, the Security Bureau has already asked all law enforcement departments under its purview to conduct urgent and comprehensive information security reviews, with a view to identifying areas for improvement. Security Bureau will undertake a coordinating function for the Law Enforcement Agencies to share experience and useful tips.

15. Mr Chairman, information security risks are constantly evolving and our approach to managing them needs to be continually improved. We need to anticipate and react to new threats as quickly as possible. The recent incidents are highly regrettable, and the Government is making sure that it addresses the risk areas that have been highlighted as effectively and as expeditiously as possible.

16. Mr Chairman, that concludes my remarks.