LC Paper No. CB(1)1540/07-08(01)
(English version only)

Remarks to be made by GCIO at the Panel on Information and Broadcasting on 13 May 2008

Mr Chairman, with your permission, I should like to say a few words about the Government's response to the recent data leakage incidents before I introduce the paper on E-government.

I am aware of the special panel meeting that has been arranged for 30 May and I do not wish to take up too much time from the important topic of E-government. However, in view of the public concern about data leakage, I though it would be desirable to inform the panel and the public about the measures that the Government is taking at the earliest convenient opportunity.

First let me emphasize that the Government takes IT security and the need to protect personal data extremely seriously. Any leakage of personal data is of grave concern to the individuals affected, even if an incident affects only a few people.

Without going into detail about the specific incidents, I can say that it appears that a significant contributing factor to many of the incidents has been lack of awareness of the established security policies and procedures, and a consequent failure to comply with them.

The Government has therefore taken immediate measures to build awareness and to assist officials to comply with the policies and procedures, and we plan to take further steps in the coming months.

The Director of Administration last week issued guidelines to all civil servants reminding them of the relevant regulations and advising them of practical means to comply. These guidelines remind officers of existing requirements and introduce some new requirements in relation to the storage of personal or classified data on portable electronic storage devices:

- Officers have been reminded to consider alternative ways of storing and accessing personal or classified data, such as working on it in its original location, or transferring it using a secure network

- Officers are now required to seek authorization from their superiors on each occasion that they consider it necessary to store data on a portable storage device
- Officers have been reminded to encrypt any personal or classified data before storage and have been provided with advice about convenient software that they can use for this purpose
- Officers have been reminded to limit the amount of personal data they store, eg by deleting items such as names and ID card numbers unless absolutely necessary for operational reasons, and by limiting the number of records and/or fields they download from a database
- Officers are reminded that portable storage devices should be used only for occasional or one-off purposes. They are now required to inform their Department IT Security Officer if they have a regular requirement, so that alternative, more secure, arrangements can be made
- Officers have been reminded that they should never store personal or confidential data on a personally-owned storage device or PC, because of the greater risk that a non-Government PC might be infected with malicious software or be exposed to other risks, such as theft

We consider that issuing this interim guidance will help to raise awareness of the need to safeguard personal and classified data, will provide officers with practical guidance on how to do so, and will reduce both the risk of future breaches and the exposure in the event that any such breach does occur.

Looking forward, we are taking a number of steps to build on the interim guidance.

First, the Government will increase the communication to all public servants with the aim of building and sustaining a high level of awareness of the security regulations, a high level of commitment to compliance with the regulations, and a high degree of awareness of how to comply in practice. OGCIO and CSB will work with Departmental IT Security Officers and Heads of Bureaux and Departments to design and implement this programme over the coming months.

Second, we are enhancing the programme of independent security audits to place additional emphasis on compliance with the regulations on use of portable storage devices. We will also ask bureaux and departments who have already been audited to provide supplementary information to confirm their compliance with these regulations.

And third, between now and the end of September, we will review IT security policies, regulations and practices in the light of the findings of investigations into the recent incidents. The review will address, amongst other things:

- Whether any changes are needed to the policies and regulations
- Whether any changes are needed to the mechanisms we use to assure that the policies and regulations are being fully implemented
- What else needs to be done to ensure a high-level of compliance, including further communications, additional training and investment in Departmental IT systems and networks

Let me conclude by emphasizing the Government's regret at the recent incidents and its determination to educate and assist officials so as to secure the greatest possible degree of compliance with our IT security regulations and hence the greatest level of security for the personal data of our citizens.