Submission to

The Panel on Security of

The Legislative Council

EDPS Systems Ltd.
28 April, 2006

In response to the invitation extended to EDPS by Hon. James To, Chairman of the Panel on Security of the Legislative Council, to discuss in the Special Meeting of the Panel on 4 May, 2006, the Independent Police Complaints Council (the "IPCC") Report on Leakage of Personal Data, EDPS Systems Ltd. would like to make the following submission to the Panel in advance:

1. The details contained in the Report do not collaborate with the statements made by Mr. Ronny Wong, Chairman of the IPCC, on 17 March, 2006 to the LegCo Information Technology and Broadcasting Panel, in which he named EDPS and OGCIO as partially responsible for the leakage.

2. The details contained in the Report do not collaborate with the untrue and very damaging statements made against EDPS by the Hon. Alan Leong, Vice Chairman of the IPCC, to the media between 17 and 22 March, 2006.

3. In spite of the above, the IPCC has not provided EDPS any apology and retraction of their statements either in this Report or through other means.

4. The Report quoted many factual details such as the contract provisions which collaborate with the EDPS' statements made to the media around 28 March, 2006.

5. The general description of the sequence of event in the Report also by and large collaborates with the description originally put forward by EDPS, although the Report made references to certain statements we disagree with.

6. After the issuance of the Report on 8 April, the media widely reported our opposing views on many points in the Report. In this submission, EDPS wants to concentrate more on the points we support and agree within the Report.

7. The evidence presented included the contracts, records of the IPCC interviews with Ms. X, the conversation between the members of the IPCC Task Force and Mr. Kirren Heung on 11 March 2006, the EDPS submissions to IPCC, and, the IPCC Secretariat internal circular 33/98.

8. Regarding the contracts, we note that the Report stated clearly in Paragraphs 2.2 to 2.4 that there is no provision against sub-contracting and no provision as to the nature of the data which EDPS would encounter.

9. Regarding the statements of Ms. X, we note in Paragraph 3.2 (e) that there is no record relating to the transfer or return of the CD containing the data for testing; and in Paragraph 3.2 (f) that Ms. X had no formal education or training in computer matters.

10. Regarding the statements from EDPS, we note in Paragraph 3.6 (c) that data was picked up from the IPCC reception for testing without any requirement to acknowledge receipt, any guidelines or safeguards; and in Paragraph 3.6 (d) that EDPS was never aware of the data was live data.

11. Regarding the IPCC Secretariat internal circular 33/98, we note that the provision of information by IPCC Secretariat is on "a definite 'need to know'" basis. This echoes Paragraph 4 of the EDPS submission to IPCC dated 22 March, 2006, in which EDPS stated that it was working specifically on the format conversion of the database records and had no "need-to-know" for the live data.

12. The "open items" of the evidence of the Report are (1) whether Ms. X told Mr. Heung the data for testing is live data, and (2) whether Mr. Heung admitted to anything in his meeting with the members of the Task Force on 11 March, 2006. However, these issues will not change the commonly-accepted evidence as listed above. As for the 2 "open items", our views are widely reported previously, and will be happy to address them again if the Honorable Councilors require me to do so when I attend the special meeting of the Panel on Security of the Legislative Council on 4 May, 2006.

13. Upon careful study of the Report, we found that the IPCC Task Force did find serious faults with its own practices in this incident, but worded Paragraphs 6.3 and 6.4 so very cleverly to disguise those faults and to apportion blame to the IT contractors, even though the Report stated in Paragraph 6.2 that "… It would not be appropriate for the IPCC … to seek to allocate blame between the initial parting of data and the ultimate rendering of access to users of the internet".

14. In Paragraph 6.3, disguised under "recommendations" arisen from Ms. X's case, the Report acknowledged in Paragraph 6.3 (a) that no confidential data should be used in IT contracts and where test data are needed, dummy data should be used; in Paragraph 6.3 (b) that the access of data should be only allowed on a "need to know" basis; in Paragraph 6.3 (c) that confidential data should be properly accounted for and protected and should not be allowed to move outside the premises of the IPCC; and, in Paragraph 6.3 (f) that the awareness of staff members of the IPCC Secretariat in data protection should be enhanced. In fact, these are indeed the issues which caused the data leakage.

15. In drastic contrast with Paragraph 6.3, the wordings and tone in Paragraph 6.4 is clear and unambiguous in its accusation of the IT contractors. I have previously argued against the 3 conclusions and the arguments were also widely reported in the press. I will just summarize to say that (1) the sub-contracting is not an issue under the contracts as described in Paragraphs 2.2 to 2.4 of the Report and is not an attributing factor of the data leakage; and (2) there are no evidence other than Ms. X's claim that any of the IT contractors are aware that the test data provided by IPCC was indeed live data.

16. The same Paragraph 6.4 of the Report contains a most unfair statement that "EDPS/Mr. Heung was the immediate and proximate cause of the data being rendered accessible to the public". Whether the same was intended or not, the inevitable impression this statement gives to the readers of the Report is that EDPS/Mr. Heung is to blame for the leakage of the secured live data. While it is uncontested that technically, there was a short-circuit in the file directory set-up, creating the unintended access path to the file folder containing what was supposed to be "dummy" or sanitized test data through the website www.china2easy.com, the fact is that EDPS/Mr. Heung did not know the data provided was in fact secured live data. The IT contractors would never have placed secured live data knowingly into such a test environment. The IT contractors would never have agreed to keep any secured live data for maintenance. Furthermore, the IT contractors would not have taken any secured live data out of the premises of the clients, and if testing or maintenance requires the handling of live data, the effort will always take place at the client's premise.

17. At most, one can say the very engineer was instrumental to or involved in what physically happened that rendered, unintentionally and accidentally, the data in question accessible via the Internet. It is a wholly different story to say that he or EDPS was the immediate and proximate *cause* of the leakage, given the other causes (regarding IPCC's mishandling of the data) imbedded and disguised in Paragraph 6.3 of the Report.

18. For those who studied the Report carefully and managed to read beyond the cleverly worded disguise in Paragraph 6.3, it should not be difficult to reach a fairer and more balanced conclusion.

We appreciate this opportunity to present EDPS' view in this most unfortunate incident and trust that our presentation on 4 May, 2006 will be helpful to the Panel.