## Senate Finance and Public Administration Legislation Committee—Additional Budget Estimates February 2007

## Answers to Questions on Notice

## Parliamentary Portfolio, Department of Parliamentary Services

## Answers to Questions on Notice

### Topic: Email protocols

### Question P10 F&PA32

**Senator MURRAY**—Do you have protocols which prevent inappropriate use of your legitimate system? Do you have a means of ascertaining whether inappropriate use has occurred? Those are the safety mechanisms you need. Obviously, in my example, the tax office did, because they could catch people, and obviously the police did in my example, because they could catch people.

**Mr Kenny**—I might have to take that on notice in terms of all the detail, particularly about what our protocols might be. However, we do have a situation where, if someone was looking at emails that they had the privilege to but it was not a requirement of their job, that would be logged as part of the normal system processes. So that access would be in there somewhere. If we discovered it then, there would be a number of things that we would be able to do, but I would have thought that an investigation for a breach of the Code of Conduct would be a starting point.

**Senator MURRAY**—What I am asking for—and you should come back to us with the answer—is this: is there a system which guarantees the integrity of your access, and, if there were inappropriate use, would it and could it be picked up?

**Mr Kenny**—The answer is that we do have the system, but I will have to get back to you on notice with the detail.

### Answer

Full administrative access to email systems is restricted to only two employees, both of whom are in positions classified as positions of trust, and both of whom have PROTECTED security clearances.

Auditing of mailbox access is possible, but is not currently done. If the auditing function is enabled, a log entry is created each time any computer account accesses a mailbox, whether it owns the mailbox or not. Due to the overhead involved in generating and storing these log entries, it is not standard practice to do so. If there was a concern about access, such as suspicion of mis-use, the auditing function could be enabled to assist the investigation.

Security logs are copied from systems for investigation purposes. DPS currently lacks the automated software tools and people to check logs routinely. Investigations would be carried out if a concern about possibly inappropriate access is raised.