ipsa
Independent Parliamentary Standards Authority

REPORT

TO: Andrew McDonald **DATE:** 14th July 2010

CC:

FROM: [redacted]

TEL:

SUBJECT: Expenses@Work System Incident Investigation

Investigation Terms of Reference:

To investigate reports from MPs that access was gained to expense claims made by other MPs in the Expenses@Work (E@W) system.

Context of the Investigation

During the morning of the 14th July 2010, it was reported by two MPs that when viewing reports and making enquiries of expense claims in the Expenses@Work system, they were able to access details of expense claims made by other MPs.

Method of Investigation

- Attempt to replicate the scenario using the MPs accounts.
- Discuss activities that may cause this behaviour in Expenses@ work with the onsite Systems@Work developer.
- Identify who has administrator access and the level of those access privileges.
- Interview users with administrator access.
- Identify who logged on to the administrator account on the morning of 14th July 2010.
- Interrogate available logs of activity in E@W system.
- Restore data from last backup to test system in an attempt to identify when the incident occurred and what information was available.

Investigation Conclusions

The attempt to replicate the incident was not successful initially and the report in question was not available when viewed through the MPs account in E@W. This suggests the incident had been rectified by 11.46am and the report was no longer available. Further

testing confirmed this and the report was no longer available when testing took place. Subsequent checks have confirmed that this report is no longer available to all users of the system and is only accessible to appropriate IPSA staff.

Access rights to all reports were reviewed and no errors or defects were detected in the E@W system.

By setting access rights to an incorrect value on the test system, subsequent attempts to replicate the incident were successful under certain conditions.

Following system testing, it was noted that administrator accounts have high-level rights resulting in the users of these accounts having the ability to modify reports in the system. Reports are normally available only to authorized IPSA staff, by modifying the report and leaving the field blank, a report will be made available to all users.

Three IPSA staff and one Systems@Work developer were working on the system in the reporting module on the morning of the 14th July; [redacted] (IPSA), [redacted] (IPSA), [redacted] (IPSA) and [redacted](systems@work).

We have concluded that one of these users accidentally removed access rights from one of the reports leaving the field blank. The E@W system does not provide an auditing facility that records changes made to reports. It is not possible, therefore, to identify exactly when the incident happened and who was responsible.

Interviews were conducted with all users but these failed to identify who may have made changes to the reporting module.

Investigation Recommendations

Immediate changes

- That changes are made to the E@W administrator accounts denying access to the modify command thereby preventing this incident being repeated.
- Introduce a two-stage process of verification so that a colleague verifies high-level administrator activity within the system.

A further report to be produced within 24 hours outlining substantial, permanent changes that will incorporate:

- Changes to the system that ensure the reports field cannot be left blank and that a mandatory flag is introduced.
- A review of access privilege levels for users and introduction of administrator activity restrictions.
- Introduction of full system auditing.
- Administrator user assessment and refresher training, if appropriate.
- Our obligations to report the incident to the Information Commissioner (ICO).