QUESTION TAKEN ON NOTICE

SUPPLEMENTARY BUDGET ESTIMATES – 20 OCTOBER 2014

IMMIGRATION AND BORDER PROTECTION PORTFOLIO

(SE14/076) PROGRAMME – Internal Product

Senator Carr (Written) asked:

With regard to the release of 10,000 asylum seekers' details, what measures have been taken to prevent this breach of privacy from happening again?
a. How will the Government ensure that this will never happen again?
b. Will vulnerability assessments be upgraded or occur more frequently?

Answer:

The abridged report by KPMG was published on the department's website on 26 May 2014. The department accepted and actioned the recommendations. An external and independent audit has been commissioned, as recommended by the Privacy Commissioner to ensure the steps recommended by both the Commissioner and the initial KPMG report have been taken.

a. The following strategies and actions have been put into place

- The major recommendation is to sanitise the data in a secure environment prior to analysis. To remove the risk of human error and address this recommendation, an automated solution has been put in place.

- Further actions have been taken to improve procedures, quality assurance and training in relation to the publishing process including strengthened policies and staff awareness.

- A high-level working group has been formed to provide formal governance for online publishing. Online publishing material has been recently updated with particular emphasis on checking for embedded or hidden data.

- Monitoring is ongoing to identify any republication of the document. To date, there has been no known instances of republication or widespread access since the department removed the document from its website.

- As part of the portfolio reform process, the department is also making significant changes to its information management practices, including separating the information management function from the ICT implementation function. This is an important organisational change which will create an internal checking mechanism to ensure the department meets its privacy obligations.