QUESTION TAKEN ON NOTICE

ADDITIONAL ESTIMATES - 25 FEBRUARY 2014

IMMIGRATION AND BORDER PROTECTION PORTFOLIO

(AE14/303) PROGRAMME – Internal Product

Senator Carr (Written) asked:

With regard to the release of 10,000 asylum seekers' details, what measures has the Department taken to prevent this breach of privacy from happening again?

a) How will the Department ensure that this will never happen again?
b) Did the department conduct a 'Penetration Test'?
c) If so, when was the last one completed?
d) What were the results/recommendations/vulnerabilities detected?
e) Were these implemented/actioned?
f) Was the Minister/Departmental Secretary aware?
g) What was the cost associated with amending these vulnerabilities?
h) If the recommendations weren't actioned, why?
i) Whose decision was this?

How will the Department ensure the safety of the 10,000 asylum seekers whose information has been released?

According to a Refugee Law expert, those who have been inadvertently exposed as a result of this privacy breach are eligible for protection on this basis alone. As such will there be any changes to the processing of these 10,000 claims?

What safeguards have been implemented on the DIBP website to ensure that access to underlying data sources will not be exposed again?

Answer:

a. The Secretary commissioned an independent review and the department commenced actions to prevent this happening again. This includes: Departmental style guides for the web have been reviewed and updated with a particular focus on attachments and underlying data management. Authors, editors and content owners have been provided with updated checklists on the preparation and checking of material prior to publication. The roles and responsibilities of those involved in the web publishing process are being reviewed and a revised governance framework is under development. This is being complemented by both face to face training for key personnel and on-line training for the balance of staff. Monitoring is ongoing to identifying any republication of the document that inadvertently might allow a savvy individual to access the underlying information. To date, this monitoring has not identified any uploading of the data beyond that identified in the KMPG report.
b. The department conducts regular "penetration testing" to guard against unlawful access to departmental systems.

c. The department completed a vulnerability assessment against the department's Internet web site in June 2013.
d. The assessment detected three relatively minor information vulnerabilities.
e. All but one of the vulnerabilities was addressed.
f. Due to the minor nature of the vulnerabilities, it was not necessary to escalate to the minister and /or Secretary.
g. The cost associated with amending these vulnerabilities was minor, they were addressed during a routine software release within the department.
h. The outstanding vulnerability was not addressed subject to a cost benefit analysis which determined that it was not an effective use of public money. The risk involved was deemed to be low while the cost of implementation high. This vulnerability did not relate to the public disclosure of asylum seekers' personal information.
i. Vulnerability assessments are signed-off by the affected Assistant Secretaries who are delegated "system owners".
j. The department has existing and robust processes in place to consider any new protection claims and that any such claims arising from the inadvertent release of client information will be considered in the process most appropriate to the person's circumstances.
k. No. The department has existing and robust processes in place to consider new protection claims including any arising from the inadvertent release of client information.
l. Please refer to the answer at paragraph (a) above.