SENATE

Penetration testing of the websites managed by the Department of Foreign Affairs and Trade (DFAT)

(Question No. 625)

Senator Peter Whish-Wilson: asked the Minister representing the Minister for Foreign Affairs on **20 May 2014**.

(1) How often is penetration testing of the websites managed by the Department of Foreign Affairs and Trade (DFAT) conducted and, specifically:

(a) are tests regular, random or a combination of both;

(b) are they undertaken by departmental officers or by external consultants; and

(c) what (if any) professional qualifications are used by DFAT to determine that those performing the required tests are capable and knowledgeable.

(2) How often is security auditing of the websites managed by DFAT conducted and, specifically:

(a) are audits regular, random or a combination of both;

(b) are they undertaken by departmental officers or by external consultants; and

(c) what (if any) professional qualifications are used by DFAT to determine that those performing the tasks are capable and knowledgeable?

(3) When was the last:

(a) penetration test conducted and did it meet Government standards as outlined in Australian Government Information Security Manual (ISM) ;

(b) audit test conducted and did it meet Government standards as outlined in the ISM

(4) Over the past 5 years have any penetration tests or security audits on DFAT-managed websites failed to meet Government standards as outlined in the ISM; if so:

(a) was the Minister at the time informed; and

(b) was client/customer data compromised in any way, both theoretically or practically.

(5) If a penetration test or security audit is found to have compromised DFAT data, what is the process for:

(a) rectifying the situation; and

(b) notifying affected people.

(6) What is the minimum Secure Sockets Layer (SSL) or Transport Layer Security (TLS) certificate version used by DFAT-managed websites?

(7) Has the Minister requested a briefing on the security of data and information on DFAT managed websites.

(8) Have any previous ministers, over the past 5 years, requested a briefing on data and information security.

Senator Brandis - on behalf of the Minister for Foreign Affairs, the answer to the Honourable Senator's question is as follows:

(1)

(a) Penetration testing on websites is conducted as part of the release process of a new web-site. It is also conducted for existing websites that are being migrated to new platforms.

(b) They are undertaken by external consultants.

(c) DFAT only engages vendors under appropriate panel arrangements who have had their skills and services endorsed.

(2)

(a) DFAT websites are protected by Australian Signals Directorate evaluated products, continuously monitored, patched regularly to remediate vulnerabilities and strictly controlled by the change process.

(b) A combination of departmental officers liaising with specialist security vendors to ensure continuous monitoring of website security.

(c) All departmental and third party vendor resources have relevant security experience and qualifications.

(3)

(a) The last penetration test conducted was for the Ministers' websites. This occurred in February 2014. Departmental web site penetration testing was conducted in late 2013. Government standards were met.

(b) We don't conduct audit tests.

(4)

(a) No test penetration tests or security audits on DFAT-managed websites failed to meet Government standards as outlined in the ISM

(b) No

(5) No DFAT managed websites have been compromised to date.

(a) Monitoring is continually conducted on web site of traffic through intrusion protection systems which block identified inbound threats.

(b) Processes are in place in case of compromise which includes ground up rebuild of systems and notification of stakeholders.

(6) All web sites use trusted 2048 bit / SHA1 versions of SSL and TLS certificates.

(7) No. However, information was provided to the Minister on how DFAT manages security and data as part of the incoming government briefings.

(8) No. However, information regarding how DFAT manages security and data was provided to Ministers as part of the incoming government briefings.