Senate Finance and Public Administration Legislation Committee —Supplementary Budget Estimates Hearing—November 2013

Answers to Questions on Notice

Parliamentary Departments: Department of Parliamentary Services

Topic: **IT Security**

Question No: **118**

Hansard Page No: 27 and 31

Date set by the committee for the return of answer: 17 January 2014

Senator LUDLAM: …What can you tell the committee about the network-level security threats posed by using Microsoft software given that it has been backdoored by foreign intelligence agencies?
…
Senator LUDLAM: …Has the parliament, and the applications and devices used by ourselves and our staff, been firewalled against use of the PRISM system in the United States?
…
Senator LUDLAM: …—or what action did you and your staff take—when those revelations became public?…When those revelations broke into the public domain, did you take any specific action?
…

Senator LUDLAM: …I am interested in the PRISM program which, effectively, bifurcates traffic and leaves a copy on the NSA servers in the United States—whether this building is immune from that collection capability or not.

Answers

What can you tell the committee about the network-level security threats posed by using Microsoft software given that it has been backdoored by foreign intelligence agencies?

There is a significant degree of speculation resulting from the Snowden revelations that a backdoor exists. Based on the available material, the speculation appears to relate to back doors in cloud related software products rather than internal environments. DPS has not been provided with any specific advice that Microsoft products or any other products have been backdoored by foreign intelligence services.

After further investigation and discussions with Microsoft and the Australian Signals Directorate (ASD) regarding backdoor exposures and PRISM:

- Microsoft has advised DPS that there is no backdoor within the Microsoft suite of products nor have they made any attempt to source information from the parliamentary network or provide information to any other entity. Microsoft has advised that they comply with all jurisdictional laws in relation to these matters;
- Microsoft advised that ASD has been a member of its Government Security Program which gives governments controlled access to a variety of Microsoft source code; and
- ASD has advised that they are not able to provide commentary on intelligence matters and that the application of the Top 35 Information Security Manual (ISM) controls remains the most effective mechanism to treat malware and advanced persistent threats.

Further advice on whether a backdoor exists or not in Microsoft products would more appropriately be directed to Microsoft itself, ASD or the “Reform Government Surveillance group”, an industry cohort of major ICT companies to address the practices and laws regulating government surveillance of individuals and access to their information.

Has the parliament, and the applications and devices used by ourselves and our staff, been firewalled against use of the PRISM system in the United States?

—or what action did you and your staff take—when those revelations became public? When those revelations broke into the public domain, did you take any specific action?

No, at this stage DPS has not been advised of a specific threat, nor has it received advice or direction by ASD that would require DPS to undertake any specific action such as firewalling or modification to our systems to stop the PRISM system.

DPS employs a number of intrusion and analysis tools to detect malware and data leakage, these tools were reviewed to determine if any malware or data leakage was evident in the environment. DPS did not observe nor detect any data leakage that would indicate the existence of a PRISM related capability.

DPS continues to implement the Top 35 ISM controls as part of its ICT security control programme. Whilst these have not been specifically designed to manage against threats such as the PRISM system, they are designed to prevent against intrusions and extraction of data from ICT systems.

I am interested in the PRISM program which, effectively, bifurcates traffic and leaves a copy on the NSA servers in the United States—whether this building is immune from that collection capability or not.

DPS Understands that the major risk would be with cloud related services where the data travels outside of Australia. What I can advise is that DPS does not host Parliamentarians' data in the cloud and that we are taking all reasonable steps to prevent systems such as the alleged PRISM system compromising our ICT environment. Our security tools have not identified any evidence of this style of illicit data collection from the parliamentary network.

DPS will continue to implement ASD controls and any reasonable recommendations that are provided by the IT industry, the Attorney General's Department or ASD to combat malware and any form of advanced or persistent threat.