QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 13 JUNE 2017

IMMIGRATION AND BORDER PROTECTION PORTFOLIO

Cyber Security Compliance – JCPAA – *Risks* - *Internal Product (DIBP)*

Chair, Asked:
CHAIR: Almost to the end. On notice, can the Department of Immigration and Border Protection just advise the committee in writing what the risks are to being able to meet the July 2018 time line that you have provided in your additional submission?
Ms Moy: We will do that.

Answer:

The Department is confident that, given the small scope of outstanding work and the resources available through the security program, full compliance with the application whitelisting strategy will be achieved by July 2018.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 13 JUNE 2017

IMMIGRATION AND BORDER PROTECTION PORTFOLIO

Cyber Security Compliance – JCPAA– *Essential Eight* - *Internal Product (DIBP)*

Mr Hill, Asked:
Mr HILL: What about the Essential Eight? Have you started any planning for the other four?
Mr Brugeaud: Yes. As part of our new Windows 10 environment, we will have the majority of our staff transitioning to that by the end of this calendar year. We will have restrictions on macros, which is an additional control in the Essential Eight, user application hardening, multifactor authentication and daily backups of data. So we are planning, as part of our—
Mr HILL: In the interests of time, perhaps you could take that on notice and send us a written response. I am just mindful that there are time constraints.

The other part of the questioning is: in reading your submission, a lot of the noncompliance, you are saying, is due to machinery-of-government issues and complexity in bringing complex systems together. Is that right?

Answer:

Question 1 -

The consolidation of the Department's technology platforms and move to a single ICT environment is a key enabler to achieving compliance with the Essential Eight.

Planning is currently underway to incorporate the additional Australian Signals Directorate mitigation strategies. These strategies are being addressed through a range of multiyear initiatives in the Department.

Since the merger of the Australian Customs and Border Protection Service and the Department of Immigration and Border Protection (DIBP), the Department operates in an environment that relies on over 500 business critical applications. Each application will be analysed in order to determine the required hardening options.

The implementation of Windows 10 and Office 2016 across the Department will mean macros are prevented from running without user approval. The Department is also investigating the use of digitally signing trusted macros to further reduce the risk of malicious macros compromising ICT systems.

The Department already requires websites to be whitelisted before they can run java applications and has implemented additional controls through network gateways to block content, including inappropriate and potentially malicious web content.

Multi-factor authentication is currently being piloted with administrative users. Following analysis of the pilot, the Department will design and implement an enterprise wide multi-factor authentication solution.

The Department already backs up all data on a daily basis and replicates the backup data to the Department’s secondary data centre.

Since the ‘Wannacry’ ransomware attack in mid-May 2017, the Department has implemented two hourly backups for its record keeping and corporate file systems.

Question 2 -

Yes. As per the Department’s submission to the enquiry, the complexity of bringing together two large, complex and vastly different ICT operating environments was identified as a contributor to the delayed compliance.

QUESTION TAKEN ON NOTICE

Parliamentary Inquiry : 13 JUNE 2017

IMMIGRATION AND BORDER PROTECTION PORTFOLIO

Cyber Security Compliance* – JCPAA – *Audit Committee – Internal Product (DIBP)

Chair, Asked:
CHAIR: Ms Bryant or the Australian tax office, how often does the audit committee meet and do any of its members have cybersecurity skills interests?
Mr Katf: Let me tackle it first. When you say the audit committee or our security committee, we have two different ones. The audit committee meets, I am pretty sure, on a monthly basis. I am not a member of that. The security committee we have also, at the moment, is meeting on a monthly basis to track a range of very important assessments and reports we have been doing, in terms of increasing our visibility and awareness and improving our processes around all of our cyber threats. That committee is made up of members of the security team and all dimensions of our security—physical security, personnel security and IT security as well as representatives from the business—to provide both the technology and security issues as well as the business perspectives of it.
CHAIR: And how does that report into the audit committee?
Mr Katf: It does provide some connectivity; there are some common members across it. The audit committee then seeks reporting—I think I am going to say on a quarterly basis but I will need to come back to you on the specifics of that.
CHAIR: Please do. And the Department of Immigration and Border Protection?
Ms Moy: In terms of cybersecurity, it is handled through the vulnerability management board. There are a number of layers between there and the executive committee. Security is a standing item on the executive committee, including cybersecurity. That is all deputies, commissioner and secretary of the department. In terms of the audit committee, I will have to come back to you on that particular issue. But the audit committee has not only the meetings where they get together and discuss the matters we are looking at, either through ANAO or internal audit, but also we work with them on an out-of-session basis, in terms of any issues that are arising as we go. And cybersecurity has been one of those issues that we have raised with them.

Answer:

The Audit Committee meets formally at least four times per year. The Chair of the Audit Committee has an interest in Cybersecurity issues and is briefed on these matters.

The Chair invites specialist advisors whenever necessary to supplement the skills of the Audit Committee members.