Response to Question on Notice

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

Cybersecurity Compliance Inquiry

Australian National Audit Office

GENERAL COMMENTS

Nil

SPECIFIC QUESTIONS ON NOTICE

Question 1

Regarding Submission 2 from Ian Brightwell:

> - One of Mr Brightwell's recommendations was to remove whitelisting from the mandatory list of strategies and focus on implementing a full set of ICT general controls to a level appropriate to the agency risk assessment. What are your thoughts on this recommendation?
>
> - Another of Mr Brightwell's recommendations is the suggestion that government Chief Information Security Officer positions not be combined within the technology delivery area and have a direct reporting line to the CEO. What are your thoughts on this recommendation? Can you please list the government agencies that have a direct CISO report to the CEO, and the government agencies that don't.

Response

The ANAO undertakes audits against frameworks set by others – the Parliament, the government and various regulators, as well as rules set by accountable authorities within their agencies. In the case of cyber security, the framework is established by the Australian Signals Directorate, with four requirements deemed as mandatory. Only three entities subject to performance audit to date have achieved compliance with mandatory requirements within the framework – AUSTRAC, Department of Agriculture and Water Resources and Department of Human Services. The ANAO offers no view on the design of the regulatory framework.

1. The governance and organisational structures of entities are matters for accountable authorities. The ANAO notes that in their responses to the recent Cybersecurity Follow-up Audit (ANAO Audit Report No. 42 of 2016–17) the:
   a. Department of Immigration and Border Protection advised that it had elevated the Chief Information Security Officer role to the Senior Executive Service Band 2 level reporting to the Chief Operating Officer, rather than to the Chief Information Officer; and
   b. Australian Taxation Office advised that it had appointed a Senior Executive Service Band 2 officer as the Chief Security Officer. This position reports to the Chief Information Officer.