JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

ANSWERS TO QUESTIONS ON NOTICE

Australian Taxation Office

24 October 2014

Topic: **Reporting processes and requirements regarding cyber security breaches**

Question: **1**

Senator LUNDY: Can I just ask each of the agencies at the table: what are your reporting requirements regarding breaches? What process do you go through when you experience either an internal or an external breach? Who do you report to and how do you handle that within your agency?

Answer:

Reporting on breaches

All ATO IT Security incident reporting is cascaded to the key operational and security committees within the ATO for full transparency and oversight. Government policy requires the ATO to report significant breaches, which the ATO does mainly through close collaboration with the Australian Signals Directorate Cyber Security Operations Centre.

Process once a breach is identified

The ATO has a strong 24x7 IT Security Incident Response program, which consists of IT security incident reporting, response and monitoring, all supported by formal processes. These processes are clearly documented, embedded within mandatory organisational policy and cascaded throughout the ATO so that the required members of the critical response team can act effectively and efficiently. The ATO's Incident Response capability has been recognised with an award from the Australian IT Security response organisation, AusCERT.