Australian Government

Department of Human Services

EXECUTIVE MINUTE

on

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT
REPORT 447

EPBC Act, Cyber Security, Mail Screening, ABR and Helicopter Program.
Chapter 5 – Cyber Attacks: Securing Agencies' ICT Systems

General comments

The Department of Human Services (the department) takes its responsibilities to manage cyber security risks seriously. The Joint Committee of Public Accounts and Audit (the Committee) and the Australian National Audit Office (ANAO) reports into *Cyber Attacks: Securing Agencies' ICT Systems* reinforced the importance and effectiveness of implementing the Australian Signals Directorate Top 4 Strategies (ASD 'Top 4') to mitigate targeted cyber intrusions as a package. To this end, the department has continued to build on established activities in implementing the ASD 'Top 4' as a matter of priority.

Response to the recommendation

Recommendation No. 8 **paragraph 5.69**

The Committee recommends that the seven agencies audited by the ANAO achieve full compliance with the top four mitigation strategies and related controls in the Information Security Manual as soon as possible.

Supported. The department has implemented a prioritised program of work to identify non-compliance and, where necessary, remediation activities are planned and completed.

Each agency should produce a clear and detailed plan of necessary activities, including a definitive date of compliance.

Supported. The department has assigned dedicated project resources to ensure the identified areas of non-compliance are remediated as articulated in the project plan.

Agencies that do not expect to achieve full compliance before August 2015 should notify the Committee – the Committee may then seek an explanation of why full compliance is not expected to be achieved, as well as the mitigation strategies the agency has put in place.

Supported. The department advises that it is currently compliant with 22 out of 27 of the mandatory controls. Four of the five remaining controls have active plans in place to achieve compliance, with compensatory controls in place until compliance is achieved in the near term. On the remaining control, the department advises that while it is not compliant for three platforms approaching end-of-life, it has ensured that alternative controls are in place to mitigate the risk to an acceptable level until these platforms are replaced.

PO Box 7788, Canberra Business Centre ACT 2610 • Telephone (02) 6223 4411 • Facsimile (02) 6223 4489
Internet www.humanservices.gov.au

The Department of Human Services

The ANAO performance report No. 50 "Cyber Attacks: Securing Agencies ICT Systems" assessed the department's overall compliance with the ASD 'Top 4', related controls and overall ICT security posture, as one of the two highest out of the agencies selected for the audit. At the same time, the ANAO noted that this was not sufficient protection against cyber attacks from external sources.

Since the March 2015 JCPAA Report, the department has completed a considerable tranche of work in its efforts to full comply with the ASD 'Top 4'. At the same time, the department has in place a number of mitigation strategies for the remaining 31 of the ASD 'Top 35' as part of a comprehensive strategy in managing the threat of cyber risks. At August 2015, the department, while not yet fully compliant with the ASD 'Top 4', is continuing its work towards full compliance as a matter of priority. There are areas where it is not possible to achieve full compliance and in these cases alternative risk mitigation strategies have been implemented so as to manage the residual risk to an accepted level. This is further explained below.

At August 2015, the department is compliant with 22 of the 27 ISM mandatory controls and 13 of the 14 best practice controls that are listed in the Australian Security Directorate's ASD 'Top 4'.

Mitigation One: Application Whitelisting

The department is fully compliant for mobile devices (excluding lap tops). It is approximately 85% compliant with Microsoft Windows workstations using a whitelisting solution known as "Applocker" which effectively blocks the vast majority of executables. Full compliance will be implemented utilising additional technology by January 2016. The vast majority (94.4%) of Microsoft servers are expected to be fully compliant in "active" mode by September 2015. The remainder are being decommissioned and this process is expected to be completed by April 2016. Other risk mitigation controls are in place to mitigate this risk in the interim.

For Unix/Linux servers, ASD has published advice to all departments on implementing application whitelisting on Unix/Linux. In addition to established controls, further strengthening of server configuration is expected to be implemented by September 2015.

Mitigation Two: Patch Applications

This is 95% compliant with vendor-supported versions for all core staff software on workstations including internet browser, email, instant messaging, Microsoft Office suite and Adobe software. Vendor-supported versions for all Enterprise server applications are in place which represent approximately 85% of all server software.

Migration plans comprising extended vendor support and/or replacement software are being progressed for a number of other server applications including a number where upgrading to the latest versions may potentially cause system outages to systems they support.

Mitigation Three: Patch the Operating System

The department is fully compliant for desktop operating systems and Microsoft Server operating systems. It is compliant for all of the mainframe operating systems in production, with the exception of one legacy system that is scheduled for decommissioning at end-of-life.

Mitigation Four: Minimise Administrative Privileges

The department is fully compliant in limiting numbers of privileged accounts allowed for the desktop environment. Monthly reviews of privileged accounts for the workstations and the Microsoft servers are performed with the results reported to the department's Risk, Business Continuity and Security Committee. For non-desktop systems where privileged access groups have been identified, there are other controls in place.

The department is compliant (with the exception of one 'partially compliant' which has compensatory mitigation controls in place) for the other ISM controls such as; administrator accounts not having access to email and not being able to access the internet, and enforced passphrase length and complexity rules for the department's workstation and server environments.

Non-compliant software platforms

Three software platforms approaching end-of-life will not achieve full compliance. Activities are underway to retire or replace/upgrade these systems, with alternative controls in place to mitigate this risk in the interim.

Alternative controls

Where full compliance with the mandatory controls has not been completed by August 2015, the department has implemented and will be reliant upon alternative but complementary mitigation strategies such as firewalls, access restrictions, and reduced number of administrators to help treat residual risks to acceptable levels. Work continues as a matter of priority to bridge any remaining non-compliant areas with dates identified for each area where applicable.

Kathryn Campbell CSC
Secretary

3 September 2015