THE HON KAREN ANDREWS MP

PARLIAMENTARY SECRETARY TO THE MINISTER FOR INDUSTRY AND SCIENCE

PO BOX 6022
PARLIAMENT HOUSE
CANBERRA ACT 2600

02 SEP 2015

MC15-001615

Dr Andrew Southcott MP
Committee Chair
Joint Committee of Public Accounts and Audit
jcpaa@aph.gov.au

Dear Dr ~~Southcott~~ Andrew

I am writing to you to provide IP Australia's response as per Recommendation 8 of the report of the Joint Committee of Public Accounts and Audit *Report 447 EPBC Act, Cyber Security, Mail Screening, ABR and Helicopter Program: Review of Auditor-General Reports No's 32-54 (2013-14)* dated 2 March 2015.

I can inform you that IP Australia has made significant progress in achieving compliance with the Top Four mitigation strategies. While a large effort has been made to achieve full compliance, IP Australia has been unable to meet the August 2015 deadline.

Applying and maintaining the Top Four for the Information Technology systems has proven a great challenge in the allotted timeframe. Despite Top Four being a high organisational priority, technical complexity and resource limits have constrained delivery. The current projected date that IP Australia will achieve Top Four compliance is 31 December 2016.

IP Australia has developed a detailed plan of necessary activities to achieve full compliance. Enclosed is IP Australia's compliance status report and summary action plan outlining IP Australia's activities to achieve full compliance by 31 December 2016.

Yours sincerely

Karen Andrews

Karen Andrews

Encl. (1)

Phone: (02) 6277 4360 Fax: (02) 6277 8462

ENCLOSURE

Summary of IP Australia's Top Four Action Plan and Compliance Status Report

Compliance Summation

Compliance is assessed against the Australian Signals Directorate's (ASD) Top Four Strategies to Mitigate Targeted Cyber Intrusion. In 2013 the Top Four were included in the Protective Security Policy Framework and government agency compliance became mandatory. The Top Four are listed in the table below.

IP Australia's compliance with the Top Four as at August 2015 is summarised in the table below for IP Australia's Information and Communications Technology (ICT) systems that have been assessed to have the highest risk. The assessment was performed in consultation with ASD.

	Very Poor				Very Good
Mitigation	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Top Four Cyber Security Threat Mitigations					
Application Whitelisting				•	
Patch Applications			•		
Patch Operating Systems				•	
Restrict Privileged Access				•	

The compliance measures in this report are expressed in the following terms:

- **Level 0**: 'Top 4' controls/alternate mitigations not in place and Agency Head has not accepted the risk for the system
- **Level 1**: 'Top 4' controls/alternate mitigations not in place but Agency Head has accepted the risk for the system
- **Level 2**: 'Top 4' controls/alternate mitigations not in place for system but agency has commenced activities to address it
- **Level 3**: 80 per cent or more of 'Top 4' controls/alternate mitigations in place for the system
- **Level 4**: 'Top 4' controls/alternate mitigations in place for the system.

Plan

- Address the remaining gaps to achieve Top Four compliance via a project with dedicated resources - **Commenced.**
- Maintain a register of ICT systems in scope for Top Four compliance and their compliance status - **Ongoing.**
- Complete implementation of monitoring and reporting against Top Four compliance – **Ongoing.**

Actions

- Amend existing contracts and agreements with ICT Service providers to include Top Four compliance.
- Finalise the recruitment of dedicated resourcing for the Top Four project.
- Implement automated checking of Top Four compliance.
- Continue to provide quarterly reporting of Top Four compliance to IP Australia's CIO and bi-annual updates to IP Australia's senior executive.

Constraints

- Continued variation of Top Four controls within the Information Security Manual as mandated by ASD – several since the implementation of Top Four became mandatory in 2013.
- Full compliance with the Top Four is resource intensive and competes with other Australian Government policy and business initiatives for budget to support research, testing, implementation and ongoing maintenance.

Mitigations

- Implementation of application whitelisting tool (Applocker).
- Application and operating system patching schedule in place.
- Admin access restricted and audited.