NATIONAL ARCHIVES OF AUSTRALIA

The National Archives submission to the Joint Committee of Public Accounts and Audit (JCPAA) inquiry into the ANAO Report No. 53 (2017-18) *Cyber Resilience*

Summary

The National Archives welcomes the opportunity to provide a submission to the JCPAA. The Australian National Audit Office (ANAO) report and recommendations on the cyber resilience of the National Archives was timely and assisted with prioritising work required to move to a cyber resilient entity and the work underway by the National Archives to develop a new whole-of-government information governance policy from 2020.

In response to the audit, the National Archives has now developed a cyber security resilience framework and a cyber improvement roadmap. Priority initiatives to improve the cyber resilience of the National Archives are progressively implemented within the affordability of the National Archives budget with executive level governance oversight.

Background

The ANAO commenced an audit in late 2017 on the National Archives to assess the effectiveness of the management of cyber risks and completed the audit in early 2018. The audit criteria included assessment of arrangements in place for managing cyber risks, monitoring of cyber security essential initiatives and the cyber resilience of the National Archives. The audit findings were formally tabled with the following recommendation for the National Archives :

- The National Archives establish a plan and timeline to achieve compliance with the Top Four mitigation strategies, and monitor delivery against that plan

The National Archives in response to the ANAO recommendation, committed to developing a cyber resilience framework and a supporting plan to effectively implement the Essential Eight. The response noted the initiatives to achieve the cyber security maturity model for the National Archives will be prioritised by the National Archives Enterprise Board taking into consideration resourcing and whole-of-government posture for cyber resilience.

Achievements to date

The National Archives placed importance of the commitment to strengthen it is cyber security maturity and has now developed and finalised the cyber resilience framework for the National

Archives and the supporting plan to progressively improve the cyber posture of the environment to move to a cyber resilient entity. The framework will underpin a secure, stable and contemporary ICT environment that supports the business of the National Archives.

The National Archives ICT practice is proactive patch Management for applications and operating systems and is aligned with Microsoft patch releases.

An action was initiated as a priority in 2018 following the audit to implement application whitelisting on windows servers. Analysis and audit mode has been completed and a phased approach has commenced to enforce whitelisting windows servers.

NAA Officer: Mr David Fricker, Director General, National Archives of Australia
Point of Contact: Ms Yaso Arumugam, Chief Information Officer, National Archives of Australia, or