Australian Government
The Treasury

TSY/AU

Submission to JCPAA

Inquiry into Cyber Resilience ANAO Report No. 53 on 2017-18

Submission to JCPAA

The Department of the Treasury (Treasury) welcomes the opportunity to provide a submission on the findings of ANAO Report No. 53 of 2017-18, Cyber Resilience, including progress on advancing the agency's cyber resilience.

1. Treasury has a strong focus on risk management and recognises the importance of cyber security to ensure its information and systems are protected and resilient. Risk management is evident throughout the department with particular effort given to security, cyber security, and high profile activities such as the Federal Budget.

2. Treasury has a strong security culture which is well supported by senior management. The security posture of Treasury is continuously improving as is evidenced by the Department reporting full compliance with the *Protective Security Policy Framework* in 2017-18. Additionally since the ANAO report was published, Treasury has:

    2.1. Reviewed and updated the full suite of security policy and process documentation for physical, protective and cyber security.

    2.2. Instigated a project to develop a comprehensive framework of security plans that has informed Treasury's future cyber security strategy.

    2.3. Implemented a centralised security monitoring and analysis platform to detect malicious activity on a wide range of Treasury IT assets.

3. Treasury has considered the recommendations made for all agencies in the scope of the audit, noting that Treasury was found to be fully compliant with the requirements of the mandatory Top Four mitigation strategies made by the Australian Cyber Security Centre.

4. Treasury will continue to monitor and manage risk associated with the Top Four mitigation strategies. The table below outlines future plans and actions.

Mandatory Controls	Future plans and actions
Application whitelisting *Finding: Compliant*	Currently evaluating tools to enhance application whitelisting and reporting capability.
Patching applications *Finding: Compliant*	Treasury has an automated mechanism to perform deployment and confirmation of application patching. Opportunities to further mature this capability will be reviewed as part of ongoing risk management.
Patch operating systems *Finding: Compliant*	Treasury has an automated mechanism to perform deployment and confirmation of operating system patches. Opportunities to mature this capability further will be reviewed as part of ongoing risk management.
Restrict administrative privileges *Finding: Compliant*	Treasury has robust controls around the issuing and maintenance of privileged user accounts. This risk is currently well managed and will be enhanced further through automation of identity management systems.

5. The audit notes that Treasury along with the other agencies in the scope had implemented only one of the four non-mandatory mitigation strategies in the Essential Eight. Treasury is actively working to mitigate risk associated with the non-mandatory mitigation strategies.

6. The table below outlines the current assessment for the non-mandatory mitigation strategies.

Mandatory Controls	Future plans and actions
Configure Microsoft Office macro settings *Finding: Not implemented*	Treasury uses Microsoft Office macros to deliver key government documents (e.g. Budget). Treasury has determined that increasing maturity with this control will negatively impact core business processes that utilise macros. Risks will be managed by the application of compensating controls delivered through desktop modernisation projects. Target for implementation: June 2020
User application hardening *Finding: Not implemented*	Treasury intends to achieve greater compliance and maturity by reducing the number of assets with third party applications installed and applying alternate controls to strengthen the environment. This work is planned as part of ICT modernisation projects. Target for implementation: June 2020
Multi–factor authentication *Finding: Not implemented*	Treasury remote access users are currently required to use multi-factor authentication. Privileged users will be required to use multi-factor authentication for administrator-level access to IT assets. Target for implementation: June 2020
Daily backups *Finding: Compliant*	Treasury has a robust and mature backup capability that includes daily backups of data, software and configurations retained for three months. Additionally, the first full backup of each month is retained for three years. Since the ANAO report, Treasury has completed a full Disaster Recovery Plan. This plan incorporates backup and recovery as part of the business process.

7. In additional to the above cyber security initiatives, the Chief Information Officer briefs Treasury's Audit Committee on cyber and IT risks. Internal audits and self-assessments provide the platform for further discussions and improve Treasury's cyber security posture.

8. Treasury actively supports portfolio agencies to improve their cyber capability. This includes risk assessments, advice on cyber and IT initiatives, and demonstrating Treasury's cyber tools and systems.

13 March 2019