Joint Committee of Public Accounts and Audit

Cybersecurity Resilience Inquiry

21 March 2019

Opening Statement by the Auditor-General

1. Good afternoon Chair and Committee Members.

2. Thank you for the opportunity to appear before the committee today, as part of the hearing based on my report No.53 of 2017–18 *Cyber Resilience* tabled in June 2018.

3. As you are aware, the audit involved three non-corporate Commonwealth entities—the Department of the Treasury, National Archives of Australia and Geoscience Australia. This hearing is about the cyber security arrangements of these three entities, and the Department of Parliamentary Services that has not been involved in any of the ANAO's cyber security audits.

4. In respect of auditing the Department of Parliamentary Services, the ANAO is developing the proposed annual audit work program for 2019. The proposed program contains a potential topic on business continuity management at the Australian Parliament House, with a focus on the Department of Parliamentary Services including its cyber security arrangements. It also contains a further potential audit of the cyber resilience of non-corporate Commonwealth entities.

5. The Committee held a hearing in June 2017 into my previous cyber security audit (Report No. 42 (2016–17 *Cybersecurity Follow-up Audit*), and subsequently released *Report 467: Cybersecurity Compliance* in October 2017. The ANAO has addressed the relevant two recommendations from that report in Audit Report No.53 of 2017–18 by examining the three audited entities' self-assessments against the mandatory cyber security requirements of the *Protective Security Policy Framework*, and outlining the behaviours and practices expected of a cyber-resilient entity.

6. The ANAO's *Insights from reports tabled April to June 2018* focused on key learnings relating to cyber resilience (https://www.anao.gov.au/work/audit-insights/insights-reports-tabled-april-june-2018), and includes a list of behaviours that may assist agencies to build a strong cyber security compliance culture and meet mandatory requirements. The Insights publication also reports the findings from the ANAO's Interim Report on Key Financial Controls of Major Entities

that in 2017–18 only 11 of 23 entities (48 per cent) self-assessed that they were compliant with what was then identified as the mandatory cyber security controls. The ANAO's cyber security audits over four years have found four of 14 entities (29 per cent) to be compliant.

7. These findings provide further evidence that the implementation of the current framework is not achieving compliance with cyber security requirements and needs to be strengthened, as proposed in Recommendation no.2 of the *Cyber Resilience* audit.

8. In this context I note that there has not yet been a response to the framework improvement focused recommendations in the Committee's *Cybersecurity Compliance* report.

9. Not implementing the mitigation strategies reduces an entity's ability to continue providing services while deterring and responding to cyber intrusions. It also increases the likelihood of a successful cyber intrusion.

10. The 2017–18 *Cyber Resilience* audit found that of the three entities:

    - Only Treasury was compliant with the Top Four mitigation strategies and cyber resilient.
    - National Archives was not compliant with the Top Four mitigation strategies but had sound ICT general controls and so was assessed as not cyber resilient but internally resilient.
    - Geoscience Australia was not compliant with the Top Four mitigation strategies and did not have sound ICT general controls so was assessed as vulnerable to cyber attacks.
    - All three entities had implemented only one of the four non-mandatory mitigation strategies in the Essential Eight, and were not well progressed in considering an implementation position for the other three strategies.

11. The *Cyber Resilience* audit found that low levels of compliance were related to entities not adopting a risk-based approach to prioritise improvements to cyber security, and cyber security investments being focused on short-term operational needs rather than long-term strategic objectives.

12. After Report No.53 was published, updates to both the *Protective Security Policy Framework* and the *Australian Government Information Security Manual* have affected the cyber security controls identified as mandatory for non-corporate Commonwealth entities. The ANAO will assess the impact of these changes on its audit work program prior to the next audit of this area.

13. We would be happy to answer any questions the Committee may have.