Joint Committee of Public Accounts and Audit

Inquiry into Cyber Resilience based on Auditor-General's Report No. 1, Cyber Resilience of GBEs and Corporate Commonwealth Entities, and No. 13, Implementation of My Health Record System

19 May 2020

Opening Statement by the Auditor-General

1. Good morning Chair and Committee Members.

2. Thank you for the opportunity to appear before the committee today as part of the inquiry into cyber resilience based on Auditor-General's Reports: –

   - No. 1 of 2019–20, *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*; and
   - No. 13 of 2019–20, *Implementation of the My Health Record System*.

3. Cyber security has been a matter of ongoing interest to the Parliament. Previous inquiries have reinforced the importance of Australian Government entities' information systems:

   - being adequately protected from both internal and external threats and attacks;
   - complying fully with mandatory Government strategies to mitigate cyber security incidents;
   - applying a strong and responsive cybersecurity strategy to protect interests from administrative efficiency to national security; and
   - being effectively implemented, alongside a corresponding enhanced security culture.

4. Past audits that have examined information systems security have shown room for improvement across the sector.

Information security, cyber security and resilience

5. The Australian Government's ability to effectively and efficiently deliver its functions relies on government entities prioritising information security. A secure cyberspace supports online activities, including information sharing and financial transactions for government, individuals

and business. Without strong cyber resilience measures there is a heightened risk to Australians' privacy as well as Australia's social, economic and national security interests.

6. The Protective Security Policy Framework is administered by the Attorney-General's Department, and refers to cyber security standards, guidance and advice provided by the Australian Signals Directorate. Non-corporate Commonwealth entities are required to apply the Protective Security Policy Framework, and implement eight essential mitigation strategies as a baseline in protecting their systems against a range of adversaries. Of the eight mitigation strategies, four are mandatory (the Top Four).

7. While not mandatory, it is good practice for government business enterprises and corporate Commonwealth entities to apply the Protective Security Policy Framework. I selected two government business enterprises and one corporate Commonwealth entity for a cyber security audit to examine how these entities were applying cyber security controls when a specific cyber security framework is not applied to them. The audit of the My Health Record also examined program specific cyber security controls in a corporate Commonwealth entity.

8. The four entities examined across these two audits had incorporated the requirements of the Information Security Manual in their cyber security risk management frameworks, and had also considered industry standards as applicable.

9. As required by sub-section 17(2) of the Auditor-General Act 1997, the Committee requested a cyber resilience audit examining the Australian Postal Corporation and ASC Pty Ltd following my request under sub-section 17(3). The audit also examined the Reserve Bank of Australia. Overall, audit report No. 1 of 2019–20 concluded that the Reserve Bank and ASC had effectively managed cyber security risks, and Australia Post had not effectively managed cyber security risks.

10. Further, while all three entities have a fit for purpose cyber security risk management framework, the ASC and the Reserve Bank met the requirements of their respective frameworks by implementing the specified information and communications technology (ICT) controls that support desktop computers, ICT servers and systems, but Australia Post did not implement all specified key controls.

11. The Reserve Bank and ASC have implemented controls in line with the requirements of the Information Security Manual, including the Top Four and other mitigation strategies in the Essential Eight. Australia Post has not fully implemented controls in line with either the Top Four or the four non-mandatory strategies in the Essential Eight.

12. The Reserve Bank and ASC are cyber resilient, with high levels of resilience compared to 15 other entities audited over the past five years. Australia Post is not cyber resilient but is internally resilient, which is similar to many of the previously audited entities. The Reserve Bank has a strong cyber resilience culture, ASC is developing this culture, and Australia Post is working towards embedding a cyber resilient culture within its organisation.

13. The report recommended that Australia Post conducts risk assessments for all its critical assets where it has not already done so and takes immediate action to address any identified extreme risks to those assets and supporting networks and databases.

14. The My Health Record audit was undertaken to assess the effectiveness of the implementation of the My Health Record system, managed by the Australian Digital Health Agency (ADHA). The audit concluded that implementation of the My Health Record system was largely effective.

15. The report concluded that risk management for the My Health Record expansion program was partially appropriate. Risks relating to privacy and the IT system core infrastructure were largely well managed, and were informed by several privacy risk assessments and the implementation of key cyber security measures. Management of shared cyber security risks was not appropriate and should be improved with respect to those risks that are shared with third party software vendors and healthcare provider organisations.

16. Two of the five audit report recommendations related specifically to cyber security, recommending that ADHA:

    - develop an assurance framework for third party software connecting to the My Health Record system — including clinical software and mobile applications — in accordance with the Information Security Manual, and

    - develop, implement and regularly report on a strategy to monitor compliance with mandatory legislated security requirements by registered healthcare provider organisations and contracted service providers.

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