Australia Post

19 March 2020

Ms Lucy Wicks MP
Chair
Joint Committee of Public Accounts and Audit
Parliament House
Canberra ACT 2600

Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20)

Dear Ms Wicks,

I write on behalf of Australian Postal Corporation (Australia Post) to assist the Joint Committee on Public Accounts and Audit (Committee) with its inquiry (Inquiry), specifically in relation to Auditor-General Report No. 1 (2019-20) *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities* (Report).

The Report made one recommendation relevant to Australia Post, 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*" (Recommendation).

Australia Post agreed with the Recommendation, whilst at the same time noting Australia Post had clear oversight of its critical asset infrastructures and had prioritised actions under a program of work already underway to address the Recommendation that involved conducting risk assessments for critical assets not yet assessed, updating assessments for those already assessed, and taking immediate action to address any concerns that are identified. Australia Post also noted that monitoring of the implementation of this program of work would be managed through our information security risk management and compliance programs, and would be reported to senior management and our Board, through its Audit & Risk Committee.

Australia Post has taken, and continues to take, steps towards implementing its program and key controls, including those evidenced during the assessment and referred to in other parts of the Report. Examples include:

- application whitelisting controls supporting its retail and deliveries environments;
- Information Security Manual accreditation for a number of Australia Post services;
- progressing its Cyber Security Resiliency project, whose scope is focused on enhancing controls on critical systems based on likely threats;
- faster detection and response to cyber incidents;

- other accreditations relating to our financial services; and
- the deliveries security uplift project, which is enhancing controls on critical deliveries systems (including whitelisting).

Since the time the Recommendation was made, Australia Post has taken the following further steps under this program of work, which is scheduled for completion by 30 June 2020:

- conducted a maturity level assessment against the Australian Cyber Security Centre Essential Eight Mitigation Strategies;
- confirmed critical application and control scope for assessment (Application scope: Business Criticality and Security ranking of critical applications; Control scope: combination of Essential Eight, Protective Security Policy Framework and risk to inform the baseline);
- conducted approach and methodology review by Australia Post internal audit;
- continued to gather source control data required to assess Applications; and
- assessed ongoing controls against Applications.

In the interests of further maturing and maintaining strong cyber resilience practices and cultures, Australia Post has since 2012 been actively working to uplift its Cyber Security maturity. Australia Post's cyber security core principles are:

- embed a business-led cyber security risk culture, including by addressing cyber security issues in material presented by management to the Australia Post Board (in addition to such issues being considered from a risk perspective at each Audit & Risk Committee meeting);
- increase coverage of fundamental security controls with targeted layering of advanced controls where required;
- adapt our cyber security services to fit different ways of working to enable our business to get to market with secure services faster;
- embed security specialists where required internally and expand external partnerships (e.g. with Law Enforcement, Government agencies, industry); and
- gain and leverage knowledge and data.

This strategy is supported by our "Securing Tomorrow" program. The program implements strategic capability uplift and the remediation of identified vulnerabilities which are prioritised through our understanding of the threat landscape, our business risks, current control maturity, external reviews and industry analysis.

We welcome the Committee's consideration of the information contained in this submission and thank the Committee for providing the opportunity to participate in the Inquiry.

For further information, please contact Australia Post's Chief Information Officer, John Cox.

Regards,

[redacted]

Christine Holgate
Group Chief Executive Officer and Managing Director