LEGISLATIVE ASSEMBLY
FOR THE AUSTRALIAN CAPITAL TERRITORY

QON No. 7

STANDING COMMITTEE ON ECONOMIC DEVELOPMENT AND TOURISM
JEREMY HANSON MLA (CHAIR), DEEPAK-RAJ GUPTA MLA, MICHAEL PETTERSSON MLA

Inquiry into referred 2018–19 Annual and Financial Reports
ANSWER TO QUESTION ON NOTICE

Asked by James Milligan MLA -

Ref: CMTEDD Annual Report, Output 1.4, Digital Strategy

In relation to: Cyber Security

1. Were there any (a) data breaches, (b) cyber-attacks or (c) any other cyber incidents, against ACT Government systems in (i) 2018-19 and (ii) 2019-20 to date?
    a. If so, advise:
        i. The date of the breach, attack or incident;
        ii. What date the breach, attack or incident was detected;
        iii. The nature of the breach, attack or incident;
        iv. What systems or data were affected;
        v. What the response from the ACT Government was at the time;
        vi. What actions were taken in response to the breach, attack or incident;
        vii. Whether it was reported to the relevant Federal Government Agencies and their response.

2. What protections are in place to ensure that all ACT Government systems are secure from cyber-attacks?
    a. How often are these systems reviewed?

Yvette Berry MLA: The answer to the Member's question is as follows:–

1. (i) During 2018-19 there were 18 incidents which were successfully mitigated by ACT Government ICT Security capabilities and were reported to Australian Cyber Security Centre (ACSC). One additional incident resulted in a data breach on an ACT Government managed system, details of this incident are as follows:

    i. The incident resulting in data breach occurred on 23 November 2018.
    ii. The incident resulting in a data breach was detected on 27 November 2018.
    iii. Several user passwords were compromised providing access to the ACT Government Outlook directory.
    iv. The ACT Government Cloud hosted directory service was affected, providing access to name and work contact details (phone number, work location, email address) of all ACT Government employees.

v. Shared Services worked with the ACSC and the Australian Federal Police to investigate, contain and remediate the incident. The investigation confirmed that there has been no compromise of any business-related systems. ACT Government staff were also notified of the data breach.
vi. Shared Services worked with the ACSC on a series of remediation steps which included the implementation of Multi-Factor Authentication for Outlook Web Access and further password protection to strengthen security measures.
vii. The incident was reported to both the ACSC and the Office of the Australian Information Commissioner.

(ii) In 2019-20 to date, 11 cyber security incidents were reported to the ACSC for reporting purposes and information sharing. These cyber incidents include common attacks like phishing and malware, all of which were successfully mitigated. None of these incidents resulted in a data breach.

2. Shared Services provides a framework of controls to help mitigate the likelihood and impacts of an adverse cyber security event from occurring to the shared ACT Government network. As enforced through the ICT Security Policy, Shared Services has aligned with the Australian Federal Government standards defined in the Australian Government Information Security Manual (ISM) published by the ACSC. This outlines a baseline cyber security framework which is used as guidance for controlling risks present in information systems, with its application of specific controls considered on a risk vs cost benefit when applied to ACT Government base infrastructure systems including standard operating environments for desktops and servers. Shared Services has also commenced implementation of the ACSC 'Essential 8' controls to mitigate cyber security incidents, these protections include:
   - patching operating systems;
   - patching applications;
   - whitelisting of applications;
   - backup/restoration capability;
   - multi-factor authentication;
   - hardening of applications;
   - macro security; and
   - restricting admin privileges.

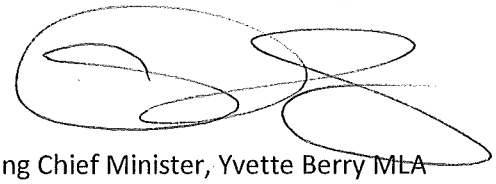
   a. Shared Services provides weekly checking of controls through automated and manual verification checking. Shared Services ICT is also subject to external verification by the ACT Audit Office as part of their Annual Financial Statement assurance process.

LEGISLATIVE ASSEMBLY
FOR THE AUSTRALIAN CAPITAL TERRITORY

QON No. 7

STANDING COMMITTEE ON ECONOMIC DEVELOPMENT AND TOURISM
JEREMY HANSON MLA (CHAIR), DEEPAK-RAJ GUPTA MLA, MICHAEL PETTERSSON MLA

Approved for circulation to the Standing Committee on Economic Development and Tourism

Signature: 

Date: 22/11/19

By the Acting Chief Minister, Yvette Berry MLA

Civic Square, London Circuit (GPO Box 1020) Canberra ACT 2601
T (02) 6205 0127 E committees@parliament.act.gov.au W www.parliament.act.gov.au