MINISTER FOR EMERGENCY SERVICES — PORTFOLIOS — CYBERSECURITY BREACHES

6321. Mr S.K. L'Estrange to the Minister for Emergency Services; Corrective Services:

I refer to each Department, Agency and Government Trading Enterprise within the Minister's portfolio of Emergency Services, and I ask:

(a) Were there any cybersecurity breaches to agency computer systems or servers in 2017;

(b) If yes to (a), for each breach:

(i) When did the breach occur;

(ii) What entity was responsible for each breach and what was their suspected purpose;

(iii) What information was compromised; and

(iv) How did the breach occur and what action has been taken to stop a recurrence of this breach;

(c) Were there any cybersecurity breaches to agency computer systems or servers in 2018;

(d) If yes to (c), for each breach:

(i) When did the breach occur;

(ii) What entity was responsible for each breach and what was their suspected purpose;

(iii) What information was compromised; and

(iv) How did the breach occur and what action has been taken to stop a recurrence of this breach;

(e) Were there any cybersecurity breaches to agency computer systems or servers in 2019; and

(f) If yes to (e), for each breach:

(i) When did the breach occur;

(ii) What entity was responsible for each breach and what was their suspected purpose;

(iii) What information was compromised; and

(iv) How did the breach occur and what action has been taken to stop a recurrence of this breach?

Mr F.M. Logan replied:

For the purpose of this response, DFES defines a security breach as a successful attempt by an attacker to gain unauthorised access to an organisation's computer systems.

(a) In 2017 no known security breaches occurred to agency computer systems or servers.

(b) (i)–(iv) Not applicable.

(c) In 2018 four known security breaches occurred to agency computer systems or servers:

(d)–(f) The State Government takes seriously any security breach or compromise of Agency data. DFES has implemented numerous cyber security enhancements consistent with the State Government's strengthening of cybersecurity, ICT performance and data sharing following the security breaches and continues to work towards improving cyber security capability. Since mid-2018 DFES has implemented an ongoing program of works to identify and mitigate risks to the confidentiality, integrity and availability of DFES information and systems.

In 2018 four known security breaches occurred to agency computer systems or servers.

<u>Breach 1 – Email compromise</u>

(i) 8 October 2018

(ii) Unknown

(iii) Email account credentials for one account

(iv) Suspect the user entered credentials into phishing website causing automated entry to their mailbox, resulting in spam/phishing emails being sent from a DFES mailbox. The user account credentials were reset.

<u>Breach 2 – Email compromise</u>

(i) 9 October 2018

(ii) Unknown

(iii) Email account credentials for one account

(iv) Suspect the user entered credentials into phishing website causing automated entry to their mailbox, resulting in spam/phishing emails being sent from a DFES mailbox. The user account credentials were reset.

Breach 3 – Email compromise

(i) 25 October 2018

(ii) Unknown

(iii) Email account credentials for one account

(iv) Suspect the user entered credentials into phishing website causing automated entry to their mailbox, resulting in spam/phishing emails being sent from a DFES mailbox. The user account credentials were reset.

Breach 4 – Email compromise

(i) 10 December 2018

(ii) Unknown

(iii) Email account credentials for one account

(iv) Suspect the user entered credentials into phishing website causing automated entry to their mailbox, resulting in spam/phishing emails being sent from a DFES mailbox. The user account credentials were reset.

In 2019 five known security breaches occurred to agency computer systems or servers.

Breach 1 – Email compromise

(i) 9 January 2019

(ii) Unknown

(iii) Email account credentials for one account

(iv) Suspect the user entered credentials into phishing website causing automated entry to their mailbox, resulting in spam/phishing emails being sent from a DFES mailbox. The user account credentials were reset.

Breach 2 – Email compromise

(i) 19 May 2019

(ii) Unknown

(iii) Email account credentials for one account

(iv) Suspect the user entered credentials into phishing website causing automated entry to their mailbox, resulting in spam/phishing emails being sent from a DFES mailbox. The user account credentials were reset.

Breach 3 – Email compromise

(i) 5 July 2019

(ii) Unknown

(iii) Email account credentials for one account

(iv) Suspect the user entered credentials into phishing website causing automated entry to their mailbox, resulting in spam/phishing emails being sent from a DFES mailbox. The user account credentials were reset, Multi-Factor Authentication (MFA) applied and credentials breach was reported through the Office of Digital Government Incident Reporting Portal.

Breach 4: – Email compromise

(i) 14 August 2019

(ii) Unknown

(iii) Email account credentials for three accounts

(iv) Suspect the user entered credentials into phishing website causing automated entry to their mailbox, resulting in spam/phishing emails being sent from a DFES mailbox. The affected user account credentials were reset, Multi-Factor Authentication (MFA) applied and credentials breach was reported through the Office of Digital Government Incident Reporting Portal.

Breach 5: – Email compromise

(i) 21 August 2019

(ii) Unknown

(iii) Email account credentials for two accounts

(iv) Suspect the user entered credentials into phishing website causing automated entry to their mailbox, resulting in spam/phishing emails being sent from a DFES mailbox. The affected user account credentials were reset, Multi-Factor Authentication (MFA) applied and credentials breach was reported through the Office of Digital Government Incident Reporting Portal.