MINISTER FOR EDUCATION AND TRAINING — PORTFOLIOS — ATTEMPTED CYBER ATTACKS

3672. Mr Z.R.F. Kirkup to the minister representing the Minister for Education and Training:

For all departments, agencies, government trading enterprises or boards within the Minister's portfolio responsibilities I ask since 11 March 2017:

(a) (a) How many attempted cyber attacks have there been on internal network systems and if any:

(i) How many of these were conducted by a non-state foreign actor;

(ii) How many of these were conducted by a nation-state foreign actor; and

(iii) How many were successful and was any material containing Cabinet or customer related detail compromised;

(b) (b) How many attempted cyber attacks have there been on external network systems or websites and if any:

(i) How many of these were conducted by a non-state foreign actor;

(ii) How many of these were conducted by a nation-state foreign actor; and

(iii) How many were successful and was any material containing Cabinet or customer related detail compromised; and

(c) (c) How many attempted cyber attacks have there been on any internet enabled devices (i.e. iPhones, iPads etc.) and if any:

(i) How many of these were conducted by a non-state foreign actor;

(ii) How many of these were conducted by a nation-state foreign actor; and

(iii) How many were successful and was any material containing Cabinet related detail compromised?

Mr P. Papalia replied:

Department of Education

(a)–(c) The Department of Education's network and online services are under frequent attack from external sources. For example, during July 2018 the Department's threat protection services detected and blocked the following:

Spoofed emails: 1,539,737

Spam emails: 466,730

Potential malware events: 20,048

Since early 2016, the Department has engaged enhanced threat intelligence and response services from an external commercial service provider. Since March 2018, the Department has experienced an ongoing series of brute force credential attacks targeting email accounts within the Department's corporate email service. These are being managed by the Department's various threat intelligence, protection and prevention services. There is no evidence that any attempts have been successful and at this time the origin of the attacks is unknown. The Department continues to work with its internal and external specialist technical security service providers to ensure that the integrity of the Department's network and online services is maintained and that the Department continues to adopt the best possible security posture.

Department of Training and Workforce Development

The Department of Training and Workforce Development detects and prevents on average 76 attacks per day. It has a number of security services including firewalls, intrusion detection and prevention systems, patch management and denial of service prevention to protect the Department from security threats. The Department's external ICT security services provide a level of protection to all TAFE colleges.

(a) Nil.

(i)–(iii) Not Applicable.

(b) Average 76 per day.

(i) Blocked unknown.

(ii) Blocked unknown.

(iii) Nil.

(c) Nil.

(i)–(iii) Not Applicable.

North Metropolitan TAFE

(a) One.

(i) Nil.

(ii) Nil.

(iii) One. Information and data that is known to have been accessed includes staff network account details, encrypted password files, computer names, IP addresses, student network accounts details including first and last name, phone, email address and in some cases addresses.

The accessed student account information did not contain current password and login credentials. There is no evidence that any student financial or banking information was accessed.

An email was sent to all affected students advising them of the possibility that some of their personal information may have been obtained. A hotline was also established to answer any student queries regarding the matter.

System security actions taken following the cyber attack were:

A staff position was created with an Information Security focus;

A sector security review occurred and remedial actions undertaken;

Remote access to the breached college system was temporary disabled following the attack and until additional security was added;

The source of the attack has been blocked at the network firewall; and

Password changes were enforced for all staff following the cyber attack and outside of the regular password change cycle.

(b) Nil.

(i)–(iii) Not Applicable.

(c) Nil.

(i)–(iii) Not Applicable.

South Metropolitan TAFE

(a) Nil.

(i)–(iii) Not Applicable.

(b) One – On 18 May 2018, South Metropolitan TAFE's website experienced an attempted cyber-attack. This was swiftly detected, and there were no adverse impacts on the college's operations.

(i) Nil.

(ii) Nil.

(c) Nil.

(i)–(iii) Not Applicable.

North Regional TAFE

(a) Nil.

(i)–(iii) Not Applicable.

(b) Nil.

(i)–(iii) Not Applicable.

(c) Nil.

(i)–(iii) Not Applicable.

Central Regional TAFE

(a) Nil.

(i)–(iii) Not Applicable.

(b) Nil.

(i)–(iii) Not Applicable.

(c) Nil.

(i)–(iii) Not Applicable.

South Regional TAFE

(a) Nil.

(i)–(iii) Not Applicable.

(b) Nil.

(i)–(iii) Not Applicable.

(c) Nil.

(i)–(iii) Not Applicable.

Building Construction Industry Training Fund

(a) Nil.

(i)–(iii) Not Applicable.

(b) Nil.

(i)–(iii) Not Applicable.

(c) Nil.

(i)–(iii) Not Applicable.