Senate Standing Committee on Finance and Public Administration

Parliamentary inquiry – Inquiry into the digital delivery of government services – 14 March 2018

ANSWER TO QUESTION ON NOTICE

Department of Defence

Topic: SRCFPA - Public hearing on the Digital Delivery of Government Services - Q1 and Q2 - Senator Patrick

Question reference number: 1 and 2

Senator: Rex Patrick
Type of question: Written
Date set by the committee for the return of answer: 4 April 2018

Question:

Can ASD provide the following information on physical and cyber intrusion attempts on Australia's networks:

1. In respect of the Government's unclassified networks (including ICON) in each of the last three financial years:
a. How many physical security intrusion attempts were detected?
b. How many were successful? (i.e. the perpetrator in some way got access to the network traffic or data);
c. How many cyber security intrusion attempts were detected?
d. How many were successful? (i.e. the perpetrator in some way got access to the network traffic or data)

2. In respect of the Government's classified networks in each of the last three financial years:
a. How many physical security intrusion attempts were detected?
b. How many were successful? (i.e. the perpetrator in some way got access to the network traffic or data);
c. How many cyber security intrusion attempts were detected?
d. How many were successful? (i.e. the perpetrator in some way got access to the network traffic or data)

Answers:

The Australian Signals Directorate (ASD) includes the Australian Cyber Security Centre (ACSC), with functions that include the development of the Government's information security manual, raising awareness of cyber security, reporting on the nature and extent of cyber security threats, analysing and investigating cyber threats, and leading the Australian Government's operational response to cyber incidents.

ASD is not responsible for the cyber security of all Australian Government networks - this remains a function of individual agencies. The Department of Finance owns and operates the ICON network. ASD does not have visibility of all Australian Government agencies' physical or cyber security postures and does not track information relating to the numbers of physical security intrusion attempts.

ASD's visibility of the broader government cyber picture is informed by survey instruments, intelligence, communities of interest, monitoring programs, cyber incident reporting and follow up investigations. The data available to ASD indicates that across the last three financial years (FY15-16, FY16-17, FY17-18), there were 1,097 cyber incidents affecting unclassified and classified government networks that were considered serious enough to warrant an operational response. ASD response is required when an incident achieves any degree of success, which can have varying impacts from significant data exfiltration and degradation of the network through to no harm being realised. The nature of the response varied depending on the incident, and ranged from telephone conversations through to deployment of staff resources and tools to assist in mitigating the incident. The data available to ASD is not categorised by the classification of the network or impact realised, and that level of detail would require costly manual review of every incident.