DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Joint Committee of Public Accounts and Audit
Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20)

2 July 2020

QoN Number: 01

Subject: Centralised Guidelines

Asked by: Tim Watts

Question:

Are there any centralised guidelines or policies for Commonwealth agencies concerning the implementation of vulnerability disclosure programs for their websites or IT systems? If not, why not?

Answer:

While there is no central policy mandating vulnerability disclosure programs, a number of Commonwealth entities have vulnerability disclosure policies appropriate to their circumstances.

Under the Protective Security Policy Framework (PSPF) the accountable authority of a Commonwealth entity must submit a report on security each financial year either through the PSPF reporting portal for information up to PROTECTED or by submitting an offline reporting template for information classified higher than PROTECTED. Each Commonwealth entity must also complete the Australian Signals Directorate (ASD) annual cyber security survey.

Additionally, a Commonwealth entity must report any significant or reportable security incident at the time they occur to the Attorney-General's Department, the relevant lead security authority and any other affected entity. This includes reporting to the Australian Cyber Security Centre in ASD cyber security incidents that relate to:

a. suspicious or seemingly targeted emails with attachments or links
b. any compromise or corruption of information
c. unauthorised access or intrusion into an ICT system
d. any viruses
e. any disruption or damage to services or equipment data spills
f. theft or loss of electronic devices that have processed or stored Australian Government information
g. denial of service attacks
h. suspicious or unauthorised network activity.

To avoid inadvertently compromising any investigation into a cyber security, Commonwealth entities are encouraged to contact the Australian Cyber Security Centre as early as possible.

DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Joint Committee of Public Accounts and Audit
Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20)

2 July 2020

QoN Number: 02

Subject: Cyber resilience education

Asked by: Lucy Wicks

Question:

The Commonwealth Cyber Security Posture (2019) outlines the importance of cyber resilience not only within Commonwealth entities but also among private business and society.

What role do policy owners in this space see for educating businesses and individuals on the importance of cyber resilience? What efforts are being taken to do this?

Answer:

Individuals, families and businesses will always carry a level of responsibility for their cyber security. The role of education is to assist individuals and business to meet the responsibility effectively. This makes awareness raising and behavior change initiatives essential complements to technical cyber security protections to reduce Australians' exposure to online threats.

The Australian Government has a number of existing awareness raising campaigns, information and advice available including:

- Cyber.gov.au (Australian Cyber Security Centre/Australian Signals Directorate)
    - Including the Small Business Cyber Security Guide
    - Stay Smart Online
- Scams Awareness Week (Australian Competition and Consumer Commission)
- Safer Internet Day (Office of the eSafety Commissioner)
- Privacy Awareness Week (Office of the Australian Information Commissioner)

The Cyber Security Strategy 2020 includes increased funding for the Government's cyber security awareness raising activities, including $4.9 million for an awareness raising campaign, $58.3 million to enhance customer engagement channels

cyber.gov.au and $38.3 million to expand the services that the Australian Cyber Security Centre provides to families, households and small businesses, such as the 24/7 cyber security hotline.