HOME AFFAIRS PORTFOLIO
DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Parliamentary Joint Committee on Law Enforcement

Inquiry into the capability of law enforcement to respond to cybercrime

14 November 2024

QoN Number: 2

Subject: Overarching strategy relating to cyber awareness

Asked by: Helen Polley

Question:

Evidence to the committee suggests there is a range of education and public awareness work underway (See Proof Committee Hansard, 16 and 22 October 2024). Is there an overarching strategy in relation to public awareness to ensure educational activities are coordinated between agencies and consistent? How is the department ensuring its messaging is effective?

Answer:

The Department of Home Affairs (the Department) works across a range of Australian Government and state and territory government agencies to ensure cyber security public awareness activities are coordinated. This is primarily managed through a number of meetings and working groups including:

- The National Cyber Security Committee (NCSC) Awareness Sub-Committee (NASC), which brings together a range of Commonwealth and state and territory government agencies to coordinate public and internal government communication and awareness raising activities in relation to cyber security to ensure consistency of messaging across Australian state/territory and Commonwealth governments.
- The Online Harms Communication Working Group, co-chaired by the Department of Home Affairs and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts, which works to assist the coordination of public messaging by Commonwealth government agencies on cyber security, online safety and the prevention of technology-facilitated abuse and cybercrime, including cyber-enabled crime.
- Regular meetings between ASD Ministerial, Media and Communication Branch and the Department's Media and Communication Branch.

The Department leads on a range of national communication and public awareness activities including Cyber Security Awareness Month and the Act Now, Stay Secure cyber security awareness campaign. The Department works closely with its state

and territory counterparts via the above working groups to amplify the key messaging and content for these major activities nationally, ensuring the delivery of a coordinated, consistent communication approach.

The Department periodically undertakes research to better understand public attitudes and behaviours towards cyber security to inform the development of messaging and public awareness activities and to ensure these are designed effectively.

The Department routinely conducts evaluations on major communication and public awareness activities to ensure these activities are effective in meeting their objectives.

HOME AFFAIRS PORTFOLIO
DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Parliamentary Joint Committee on Law Enforcement

Inquiry into the capability of law enforcement to respond to cybercrime

14 November 2024

QoN Number: 3

Subject: Cyber incident reporting portal

Asked by: Helen Polley

Question:

As noted by National Cyber Security Coordinator (Proof Committee Hansard, 22 October 2024, p. 40), an initiative under the 2023–2030 Australian Cyber Security Strategy Action Plan is for a single reporting portal for cyber incidents.

(a) Would this portal be only for businesses affected by a cyber incident? Or would it be available to individual victims of cybercrime?

(b) How would the portal relate to existing reporting mechanisms, including ReportCyber, Scamwatch, and reporting online harm to eSafety?

Answer:

The Single Reporting Portal is a multi-phase initiative within the *2023-2030 Australian Cyber Security Strategy* (the Strategy) seeking to simplify reporting requirements for entities experiencing a cyber incident. Phase One of the Single Reporting Portal was delivered alongside the launch of the Strategy in November 2023, and is currently available on cyber.gov.au.

(a)
The Single Reporting Portal is seeking to make it easier for businesses impacted by a cyber incident to meet their mandatory regulatory reporting obligations. Individuals who are victims of cybercrime are not within the scope of this initiative.

During the development of the Strategy, the Australian Government consistently heard that the current regulatory reporting requirements for cyber security can be complex and varied – depending on an entity's sector and size, and the type of incident that has occurred.

Industry detailed, when responding to a serious cyber incident, an organisation needs to triage the incident; assess the damage, including impact; and comply with mandated reporting requirements. This can include reporting to multiple regulators, and against differing timeframes based on the affected entity's sector. This results in multiple reports to different regulators, where the information provided can often be duplicative.

The Single Reporting Portal initiative will explore options to make it easier for entities affected by cyber incidents to meet their mandatory regulatory reporting obligations. These options may include regulatory harmonisation, form simplification and streamlined reporting.

(b)
The final design of the Single Reporting Portal – including any changes to, or interactions with, existing cyber incident and online harms reporting mechanisms – is a matter for Government. The Department will lead consultation with relevant departments responsible for administering reporting portals including ReportCyber, Scamwatch and eSafety.