Question No: 153

The Australian Communication and Media Authority

Hansard Ref: Page 18-19, 25/05/2016

Topic: Cybersecurity programs – transfer to the Attorney-General's Department

Senator Urquhart, Anne asked:

Senator URQUHART: Minister, given the government's support for the cybersecurity programs being transferred to the A-G's Department, do you think there is a risk that stakeholders will experience a less harmonised approach from government? Is there a risk of greater duplication and red tape for stakeholders in the cybersecurity space?

Senator Fifield: I do not think that is the case, Senator. I might just take you through what the division of labour is in relation to cybersecurity matters, which we touched on during the discussion with the eSafety Commissioner. It is a multilayered thing. The online environment is not owned by any individual agency, so I will just take you through the various elements. Cyberthreats and vulnerabilities—I guess matters in relation to that are broader policy issues for the Special Adviser to the Prime Minister on Cybersecurity. Questions about online crime fall to the Australian Federal Police. Matters relating to terrorism or the financing of terrorist organisations through online advertising are matters for the Attorney-General's portfolio and the Australian Federal Police. Questions relating to online privacy are for the Office of the Australian Information Commissioner. Questions relating to online scams are matters for the Australian Competition and Consumer Commission. As we have noted, ACMA's cybersecurity program is being transferred to the Attorney-General's Department. So those are the broad jurisdictional arrangements for the online environment.

Senator URQUHART: Are you able to table that detail or provide it?

Senator Fifield: We will provide that. It is in a scribble format, so we will provide—

Senator URQUHART: Tidy it up for me—thank you.

Answer:

This question has been answered using input provided by the Department of Communication and the Arts (the Department) which consulted with the Australian Communications and Media Authority (ACMA), the Department of Prime Minister and Cabinet (PM&C), the Attorney-General's Department (AGD), the Australian Federal Police (AFP), the Office of the Australian Information Commissioner (OAIC) and the Australian Competition and Consumer Commission (ACCC).

- *Australia's 2016 Cyber Security Strategy* explains that Australia's cyber security policy governance is overseen by the Special Adviser on Cyber Security, and the Department of Prime Minister and Cabinet has responsibility for cyber security policy matters.

Senate Standing Committee on Environment and Communications
Answers to Senate Estimates Questions on Notice
Budget Estimates May 2017
Communications Portfolio
Department of Communications and the Arts

- The Special Adviser to the Prime Minister on Cyber Security is responsible for driving implementation of the Strategy and is responsible for leading cyber policy across the Commonwealth.

- The AFP plays a significant role in maintaining a safe and secure online environment; this includes investigating cybercrime matters that fall within this remit and helping raise cyber safety awareness. The AGD helps to develop domestic cybercrime policy and criminal law more generally

- AGD also hosts Australia's Computer Emergency Response Team – CERT Australia – which provides advice and assistance to help Australian businesses mitigate malicious cyber activity.

- The Office of the Australian Information Commissioner has three primary functions which include the online environment: privacy; freedom of information; and government information policy.

- As part of its broader consumer protection role the ACCC maintains the Scamwatch website which aims to assist people to recognise scams and avoid them where possible. Scamwatch provides information and educates the public about a range of scams including online and phone based scams.

- The Australian Internet Security Initiative (AISI) helps minimise the cybersecurity threat to Australian internet users by providing Internet Service Providers and other AISI partners (including educational institutions) with daily reports listing malware infections and vulnerable services and devices in their networks. The AISI transferred from the Australian Communications and Media Authority to the Attorney-General's Department on 1 July 2017 as recommended by the ACMA review final report.

- The ACMA retains responsibility for spam and phishing. This is as ACMA's phishing alert service and spam public awareness website activities are closely linked to spam reports received by the ACMA that arise from its regulatory responsibility under the *Spam Act 2003*. Given this, the ACMA and AGD have agreed that the spam and phishing functions will remain with the ACMA due to its ongoing regulatory role in these two activities.