

INQUIRY QUESTION

(Question No. 1)

Senator Helen Polley asked the Australian Signals Directorate the following question, upon notice, on 04 June 2024:

It was suggested to the committee that there is a need to analyse ReportCyber reports to find shared characteristics and identify reports that may relate to the same criminal group or scam (*Committee Hansard [Proof]*, 23 May 2024, p. 23).

- Can you please advise what level of analysis is done on reports to detect patterns?
- Does the analysis also consider reports made to the National-Anti-Scam Centre via ScamWatch?
- How is this analysis shared to inform law enforcement's response to the reports?

Australian Signals Directorate provides the following answer:

- Can you please advise what level of analysis is done on reports to detect patterns?
 - ASD conducts trend analysis and produces alerts, advisories and publications based on the reporting it receives through www.cyber.gov.au and the Australian Cyber Security Hotline (1300CYBER1). This data underpins the ASD Annual Cyber Threat Report, which is available at www.cyber.gov.au. The trend analysis is also made available to law enforcement agencies to inform products such as the Australian Institute of Criminology's publication 'Cybercrime in Australia 2023'.
- Does the analysis also consider reports made to the National-Anti-Scam Centre via ScamWatch?
 - No, as this data is not received by ASD.
- How is this analysis shared to inform law enforcement's response to the reports?
 - State and Territory law enforcement, and the Australian Competition and Consumer Commission, through the National Anti-Scam Centre, have access to ReportCyber data that is relevant to their jurisdiction and function. The AFP maintains access to the overall ReportCyber data and contributes to the development of the ASD Annual Cyber Threat Report. AFP and ASD operationalise insights from ReportCyber through joint standing Operation Aquila.