

QUESTION TAKEN ON NOTICE

JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT – REVIEW OF AUDITOR GENERAL'S REPORTS 42-43, 48, 50 AND 52

IMMIGRATION AND BORDER PROTECTION PORTFOLIO

AUSTRALIAN CUSTOMS AND BORDER PROTECTION SERVICE

Senator Lundy asked:

Can I just ask each of the agencies at the table: what are your reporting requirements regarding breaches? What process do you go through when you experience either an internal or an external breach? Who do you report to and how do you handle that within your agency?

Answer:

The Australian Customs and Border Protection Service (ACBPS) operates a proactive Security Operation Centre (SecopsCen) which utilises a range of specialist security tools integrated into a Security Information & Event Management (SIEM) system. This system is based on similar technology and processes used by the Australian Signals Directorate (ASD) Cyber Security Operations Centre (CSOC).

In all cases the incident is advised to the ACBPS Strategic Border Command Centre who assesses the incident in the context of national border security operations. The ACBPS SecOpsCen is the single source of truth for all reported or detected security incidents, not just cyber incidents.

The ACBPS has close collaboration with the ASD CSOC on matters that relate to vulnerabilities, threats, methods and practices. This close collaboration with ASD provides the ACBPS with expert guidance and or resources to assist with the matter.