



Australian Government Agencies Fail in Setting the Example in Cyber Security: Accountability Measures Needed

Media Release: 19 December 2022

Researchers in the Social Cyber Group are calling for greater accountability of department heads in Australian government agencies in the national security portfolio for continuing failure in some basic measures of cyber protection, after a new report by the Australian National Audit Office (ANAO).

'As the Australian public grapple with the catastrophic cyber security breach in Medibank, they would reasonably expect government agencies to set the example with the highest cyber security standards, but this is not yet happening', according to Professor Glenn Withers, co-founder of the Social Cyber Group.

Dr Greg Austin, also a co-founder of the Social Cyber Group, observed that 'the lack-lustre performance of government agencies in cyber security at a time of increasing state-on-state attacks, including those arising from the war in Europe, is a threat to our national security'. He added that "Minister Clare O'Neill, whose Department for Home Affairs is responsible for cyber security, must now act on the succession of ANAO reports finding specific government agencies to be so consistently deficient in basic cyber security."

The Social Cyber Group calls on the Australian government to devise effective measures to bring its agencies more rapidly into line with fundamentals of cyber security. This would almost certainly need to include penalties for agency heads who oversee the continuing shortcomings.

Background: In a [report issued on 14 November 2022](#), the Australian National Audit Office (ANAO) found that the Department of Foreign Affairs and the Australian Federal Police have fallen short in meeting basic standards in cyber security for supply chain assurance. They "do not manage compliance of contracted providers with the PSFP requirements for cyber security", the report said. (PSFP is the government-mandated Protective Security Policy Framework.) Cyber security is one of the most important aspects of Australian government administration that causes the Auditor General concern, he said in his [last annual report](#). The critiques by ANAO of the cyber security performance of key government agencies began in 2014. The 2021-22 annual report identified "optimism bias in reporting by entities, and little analysis or escalation of the success or otherwise of the policy framework to government".

In response, the Social Cyber Group's Institute recently released [a six-point plan for reform of Australian cyber security](#), for which Dr Austin is the lead author.

Contacts

Business and Media: Lisa Materano +61 438134558
Reform Plan Lead Author: Greg Austin +61 450190323