Media contact: Natasha Farrell
Mobile: 0427 953 993
Email: natasha.farrell@audit.wa.gov.au

6 December 2023

State government entities need to do more to protect sensitive information and critical service delivery from cyber threats

State government entities still need to do more to fully implement essential baseline cyber security controls to protect systems and sensitive information from malicious attacks.

The Auditor General's report, *Implementation of the Essential Eight Cyber Security Controls* tabled in Parliament today.

It examined the progress made by 10 State government entities to implement the Australian Signals Directorate's Essential Eight cyber security controls and the accuracy of their self-assessments reported to the Office of Digital Government (DGov).

'Essential Eight' are the baseline security controls to mitigate and protect against cyber security threats, which include multi-factor authentication, regular backups and restricting administrative privileges.

Auditor General Ms Caroline Spencer said recent cyber attacks have highlighted the need for cyber security to be a key strategic priority across the public and private sectors.

'The 10 audited entities provide a range of essential services to the Western Australian public and hold large amounts of sensitive and personal information.

'We found many controls were only partially implemented or not working as expected, leaving entities vulnerable,' Ms Spencer said.

'Weaknesses in an entity's cyber security leave it exposed to the threat of data breaches, unauthorised access and disruption to their systems and services.'

'While I recognise that upgrading or replacing large legacy systems takes time and often requires significant planning and resources, it is critical this work continues in order to avoid interruption to service delivery to the public.

Further, most entities were overly optimistic in completing their Essential Eight maturity self assessments. Controls at seven entities were not as mature as they had self-assessed and reported to DGov, formed by the WA government to build cyber security capabilities of State entities.

'This presented an inaccurate and overconfident picture of their own readiness but also the public sector's cyber resilience.

Entities need to have an accurate understanding of their maturity to prioritise and address weaknesses, and correctly inform the government's perception of the State's cyber risk exposure.

'It is not uncommon for entities to be overconfident when self-assessing, a trend noted by other jurisdictions in Australia,' Ms Spencer said.

As entities deliver important services to the public through internet-facing systems, they can be subject to attacks. Further, a secure digital environment is vital to Australia's national interest, social confidence and cohesion, and economic prosperity.

’Pleasingly, DGov is aware of the issues impacting the accuracy of entity self-assessments and has already commenced a review of its guidance and tools to assist entities to more accurately assess their maturity.

‘The government is increasingly focused on cyber security and is continuing to build the skill base and digital resilience across the public sector.

Report resources

- PDF version
- summary video