National Office of Cyber Security,
Department of Home Affairs.

29 August 2025

Lodged via webpage

Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Australian Payments Plus (**AP+**) are strong supporters of the Government's 2023-2030 Australian Cyber Security Strategy, which seeks to build national cyber resilience and boost cyber security across the economy. We support the Government's focus to ensure that Australia's regulatory, legislative and policy settings seize the opportunities of technological advancements, while protecting our national interests.

AP+ was created when Australia's domestic payments companies – BPAY Group, eftpos, and the New Payment Platform (NPP), merged in 2022, and which subsequently launched the digital ID ecosystem, ConnectID. Our payment schemes are subject to Reserve Bank of Australia (RBA) oversight under the Payments Systems (Regulation) Act and the Security of Critical Infrastructure Act (SOCI), and ConnectID is an accredited entity under the Digital ID Act.

AP+ observe the requirements of ISO 22301:2020 Security and Resilience and undertake ISO 27001:2022 assurance and certification.

Horizon 2 consultation

Given our role as the operator of Australia's payment and identity exchange infrastructure, we have considered the objectives of this Horizon 2 consultation and have several recommendations that relate to *Shield 1 Strong businesses and citizens* and *Shield 4 Protected critical infrastructure.*

Greater use of Digital Identity to drive data minimisation

The discipline of data minimisation across all entities in the economy is a key mitigation of cyber risk and helps to achieve several outcomes expressed in the Cyber Security Policy Evaluation Model. An organisation known to be holding less data is a less attractive target for Australia's adversaries. Where breaches do occur, data minimisation reduces the impact stolen identity data has on citizens and reduces remediation costs for businesses and governments.

The Government's Cyber Security Strategy should leverage Australia's Digital ID System, to increase Australia's resilience to cyber threats and identity fraud, across the economy. Governments, private industry and citizens all have a role to play in protecting privacy and data in this digital age.

Uplifting critical infrastructure resilience

The SOCI Act is driving tangible uplift in the cyber security and operational resilience of Australian critical infrastructure. Current obligations are proportionate as SOCI is principally risk-based and offers responsible entities optionality in their chosen cyber security framework.

The Government should continue to engage industry as updates to the monitoring and enforcement framework are considered as part of Horizon 2, specifically in the development of sector-specific measures and activities to increase maturity to requisite standards. Consideration needs to be given to the practicality and effectiveness of any mandated requirement so that the regulatory burden remains proportionate to the risk and outcomes being sought.

The Government can double down on several initiatives to further assist infrastructure owners and operators to mature cyber and operational resilience. Though published guidance is helpful, some organisations lack the technical skills or resources to implement it. Expansion to initiatives like ACSC's Critical Infrastructure Uplift Program (CI-UP) can assist in filling the gap. Additionally, PSPF Directions are a strong signal to the private sector and can help cut through the noise or ambiguity in guidance. As the government gets greater visibility of technology risk across its digital estate and the private sector, PSPF Directions could be used more frequently to encourage a prompt response in eliminating security antipatterns.

Australia's regulatory, legislative and policy settings

Cyber security policy cannot be considered in isolation. It will be more effective working in conjunction with secure data sharing and identity proofing regulation across the economy. Challenging examples include specific government agency policies (such as those which require a 100 point check), or sector-based regulations such as AML/CTF, telecommunications, or rental regulations, which essentially enshrine oversharing of data or government documents.

Additionally, guidance from all federal and state regulators to encourage better data practices to minimise data collection, and encourage the uptake of more secure technologies like digital identity would be valuable.

An example of work being done to address the issue in a secure, citizen-friendly manner is the Department of Finance's pilot program, using digital ID and the Consumer Data Right in the context of residential rental applications. An outcome where real estate agents are no longer storing government documents and payslips is an improvement in Australia's data resilience.

We note the request for ideas on initiatives across multiple levels of government which could be replicated. The Data and Digital Ministers Forum, chaired by Senator the Hon Katy Gallagher, is an example of how Home Affairs could encourage the building of data resilience across the economy. The Data & Digital Ministers Forum includes ministerial representation from all Australian states and territories, and New Zealand, and is an excellent example of cross-government collaboration on data and digital transformation to ensure smarter service delivery and improved outcomes.

We are available to discuss our submission with the Department.

Yours sincerely,

[redacted] [redacted]