PEXA Submission

Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

29 August 2025

Property Exchange Australia Limited | [redacted]

PEXA welcomes the opportunity to provide its feedback on the Australian Government's Policy Discussion Paper, *Charting New Horizons - Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy*.

PEXA has participated in previous consultations on the development of the *2023-2030 Australian Cyber Security Strategy* (**the Strategy**), and subsequent related consultations including the 2024 legislative package.

PEXA is an Electronic Lodgement Network Operator (**ELNO**) approved to operate across all Australian states and territories, enabling electronic conveyancing and the transfer of real property through its platform, the PEXA Exchange. PEXA works closely with its integrated network partners, including financial institutions, land registries and state revenue offices, to improve the overall cyber security posture of the electronic conveyancing ecosystem. PEXA's customers comprise more than 160 financial institutions, 345 government bodies, and over 10,000 conveyancing and legal practitioners who represent high-priority targets for cyber criminals given their role in handling significant funds associated with property transactions. Developing resilience within this sector is essential to addressing the evolving, and often sophisticated, cyber security threats encountered by Australians. As the operator of a critical infrastructure asset, PEXA performs a pivotal role in driving and supporting this development.

PEXA maintains its position of prior submissions to this Strategy (and subsequent consultations) that industry Regulators must be equipped with requisite technology skills in the context of the sectors which they oversee. By extension, technology competency should lend itself to increased appreciation of cyber security risks and, consequently, broader consideration of the impacts which sector-specific reforms may have on achieving, or impeding, objectives of the Strategy, including the regulation of critical infrastructure.

In respect of ***Shield 4***, specifically the focus area '*Maturation of our regulatory framework for critical infrastructure security'*, PEXA supports the continuation of the Government's role in ensuring that the cyber security of Australia's critical infrastructure is appropriately protected and secured through regulatory schemes. However, in supporting the aim for Australia's critical infrastructure owners and operators to play a leading role in strengthening national cyber resilience by 2028, we provide the following feedback:

(1) Other arms of government hold different priorities which do not always complement the objectives of the Strategy or SOCI Act. Within the electronic conveyancing industry, state governments and some Commonwealth bodies have pursued competition reform in the form of interoperability. While interoperability has served some digital markets, its application must always take into account the unique circumstances of the industry, market, or platform, it relates to. In PEXA's view, the

push to introduce interoperability for electronic conveyancing, now in its 7th year with no foreseeable implementation timeframe, risks compromising security outcomes as pressure mounts on stakeholders to deliver this reform.

While security has been established as a core principle of the reform, it has become less of an imperative with the industry regulator, ARNECC, since announcing a cost-benefit analysis that will assess several models, some of which have not yet been defined. If the perceived economic benefits of any one of those models is enthusiastically adopted by policymakers, concerns around cyber security, such as broadening the attack surface of the network, are at risk of being discounted and not factored into the 'costs' of the reform.

This cost-benefit analysis is to be undertaken in the context of two Parliamentary Inquiries – separately held in the NSW and Commonwealth Parliaments. PEXA will advocate against measures that may impact cyber security and will remind policymakers that governments, across all levels, share a common interest in fulfilling the objectives of the Cyber Security Strategy. We recommend the Department of Home Affairs engages with these Inquiries also.

(2) In providing paths for industry to mature their respective cyber security levels, legacy frameworks should be evaluated to ensure they are not prohibiting such development. An example faced by the electronic conveyancing industry relates to the Gatekeeper Public Key Infrasturcture Framework. Proper authentication of participants to an electronic conveyancing transaction is essential, and this is supported through a digital certificate regime where the certificates used by those participants, and validated by the ELNO, must be issued by Gatekeeper-accredited organisations.

The Framework was first developed in the 1990s to support contemporary policies which are now defunct. However, industry regulators such as ARNECC continue to rely on the Framework as a marker of best practice. While Gatekeeper maintains it merits, the uptake of accreditation by digital certificate providers has not been strong and is presently regressing. Consequently, industry's dependency on a shrinking list of accredited providers limits its capacity for continuity planning and therefore resilience.

While other frameworks may serve as suitable supplements or replacements, there is understandable reluctance by regulators to adopt or endorse those frameworks without leadership from higher authorities, including the Commonwealth Government and architects of this Strategy. PEXA has been informed the Gatekeeper Framework is

currently under review and that accreditation of new providers has been paused. We encourage the Department of Home Affairs to engage with this review (led by the Department of Finance) in respect of assessing barriers which may impede the maturation of the regulatory framework for critical infrastructure security.

(3) Lastly, PEXA has encountered difficulties associated with disclosing sensitive information to other critical infrastructure stakeholders, as may be required by those organisations in accordance with their own sector's regulatory framework, such as CPS 230 for APRA-regulated entities. Industry regulators may, from time-to-time, introduce or amend requirements for the regulated entity to seek and obtain confirmation of cyber security practices undertaken by their material suppliers (third and fourth parties). In doing so, the onus on that material supplier, who may operate a critical infrastructure asset themselves, and is therefore subject to the SOCI Act, is conflicted by such obligations to disclose the relevant information. To the extent these conflicts are capable of being resolved, PEXA considers this worthy of further investigation under Shield 4 of Horizon 2.

PEXA once again thanks the Australian Government for this opportunity to provide feedback on its Policy Discussion Paper and looks forward to further development of the Strategy. PEXA is available to discuss its experiences and feedback further with the Department of Home Affairs and other policymakers.