Australian Government
Department of Home Affairs

Department of Home Affairs submission to the Inquiry into Micro-Competition Opportunities

Senate Economics Reference Committee

25 September 2025

Table of Contents

Introduction

The Department of Home Affairs welcomes the opportunity to provide input to the Senate Economics References Committee inquiry into micro-competition opportunities.

The Department has policy and administrative responsibility for the *Security of Critical Infrastructure Act 2018* (SOCI Act), which provides the legislative framework for strengthening the security and resilience of Australia's most essential infrastructure assets. The SOCI Act applies a targeted and proportionate set of obligations to the responsible entities for critical infrastructure assets, with a focus on ensuring the continuity and security of systems and services that underpin Australia's national interest against all hazards.

These obligations are structured around 11 sectors and 22 asset classes, including electricity, telecommunications, financial markets, public transport and data storage or processing assets. An asset is brought within the scope of the SOCI framework when it meets the definition of a critical infrastructure asset under the SOCI Act, or is otherwise declared as such by the Minister for Home Affairs.

The Department does not administer the regulatory frameworks governing electronic conveyancing, and we have no role in assessing market structure, pricing or competition policy. As such, the Department's comments within this submission are limited to the question of how the SOCI Act may apply to electronic lodgement network operators (ELNOs) such as Property Exchange Australia (PEXA).

Regulation under the SOCI Act

Sector and asset class coverage

There are no sector or asset classes relating specifically to ELNOs. The PEXA Exchange is regulated under section 12F of the SOCI Act as a critical data storage or processing asset. This asset class applies across multiple sectors and service types; it is not tied to any particular industry or entity.

- An asset falls within the scope of section 12F where:
  - it is owned or operated by an entity that provides a data storage or processing service
  - the asset is used wholly or primarily to provide a data storage or processing service that relates to "business critical data" and is provided to an end-user that is:
    - the Commonwealth (or a body corporate established by a law of the Commonwealth), or a State or Territory (or a body corporate established by a law of a State or Territory); or
    - the responsible entity for another critical infrastructure asset
  - the entity knows that the asset is used as described above, and
  - the asset is not already covered as a different type of critical infrastructure asset
- 'Business critical data' is defined in section 9 of the SOCI Act as:
  - personal information (within the meaning of the Privacy Act 1988) that relates to at least 20,000 individuals
  - information relating to any research and development in relation to a critical infrastructure asset
  - information relating to any systems needed to operate a critical infrastructure asset
  - information needed to operate a critical infrastructure asset; or
  - information relating to risk management and business continuity in relation to a critical infrastructure asset.

Regulatory obligations

Once an asset is captured under the SOCI Act, its responsible entity is subject to a range of obligations designed to enhance security and resilience and reduce the risk of disruption. Generally, a critical data storage or processing asset may be required to meet the following requirements, amongst others:

- **Register obligations (Part 2 of the SOCI Act)**: responsible entities and direct interest holders must provide ownership and operational information for the asset to the Register of Critical Infrastructure Assets, which is managed by the Department.
- **Critical infrastructure risk management program (Part 2A of the SOCI Act)**: responsible entities must develop and maintain a critical infrastructure risk management program (CIRMP) that addresses cyber, physical, personnel and supply chain risks. This obligation requires the responsible entity to consider all hazards and risks that may have a relevant impact on the availability, integrity, reliability or confidentiality of the asset and, where reasonably practicable, minimise, mitigate or eliminate them.[1] Section 30AG of the SOCI Act establishes a reporting requirement on the entity, requiring the entity to submit an annual report addressing a number of matters relating to their compliance with their CIRMP obligation within the defined reporting period.
- **Mandatory cyber incident reporting (Part 2B of the SOCI Act)**: responsible entities must report certain cyber security incidents affecting their asset/s to the Australian Signals Directorate's Australian Cyber Security Centre (unless specified otherwise).
- **Enhanced cyber security obligations (Part 2C of the SOCI Act)**: where an asset is declared a System of National Significance (SoNS), the responsible entity may be subject to additional requirements including incident response planning, cyber security exercises, and vulnerability assessments.

In addition to the positive security obligations outlined above, the SOCI Act provides the Government with a set of last resort powers under Part 3 and Part 3A of the legislation. These powers are designed to be used in exceptional circumstances, where there is a significant threat to Australia's national interests and other regulatory levers are insufficient or unavailable.

Under Part 3, the Minister for Home Affairs may issue directions to the responsible entity for, or an operator of, a critical infrastructure asset to do, or refrain from doing, an act or thing, if the Minister is satisfied that there is a risk of an act or omission that would be prejudicial to security. The exercise of this directions power is subject to rigorous thresholds and safeguards, as outlined in section 32 of the SOCI Act.

Part 3A establishes the government assistance measures framework, which enables more direct intervention by the Government to respond to a serious incident that has had, is having, or is likely to have, one or more relevant impacts on one or more critical infrastructure assets. This includes the power to:

- request information to assess the risk or impact of an incident
- assist the entity in responding to or remediating the incident; and
- as a last resort, authorise the Australian Signals Directorate to step in to provide assistance directly on an entity's network or systems.

These powers are designed to protect the Australian community and economy from cascading or systemic risks in situations where a critical infrastructure asset is unable or unwilling to respond effectively on its own. The powers can only be exercised as a matter of last resort and only where no existing regulatory mechanism can be used to address the incident. The government assistance measures have not been used to date.

For entities like PEXA, whose platform supports essential financial and property settlement processes across nearly all state and territory jurisdictions, this capability ensures that the Government can respond decisively if our national security or social or economic stability is at stake.

[1] Responsible entities may be exempt from the CIRMP obligation if the entity holds a certificate of hosting certification (strategic level) relating to one or more services and where other conditions are met.

Ensuring resilience in e-conveyancing platforms

The Department notes that the Committee's inquiry has raised concerns regarding PEXA's market position and the risk that it could represent a single point of failure for property transactions in Australia. The Department acknowledges that the scale and concentration of PEXA's services increase the criticality of the functions it performs. Outages within the PEXA Exchange could delay settlements and foreseeably cause significant downstream impacts during a severe incident. This exposes the fundamental interconnectedness of Australia's critical infrastructure.

The obligations in the SOCI framework outlined above, particularly those under the CIRMP, are specifically designed to mitigate these risks. The CIRMP creates a legislative requirement for entities to embed risk management at the core of their business operations. It requires entities to proactively consider and manage risks across the four identified domains, together encompassing 'all-hazards', to ensure the resilience and security of their asset. The CIRMP also requires responsible entities to meet a minimum cyber security framework.[2]

Beyond the legislative framework, the Department also facilitates industry-government collaboration through initiatives such as the Trusted Information Sharing Network (TISN). The TISN enables trusted engagement between critical infrastructure owners and operators and Government to build a shared understanding of threats and uplift collective resilience. ELNOs regulated under the SOCI Act are encouraged to participate in this forum to support cross-sector maturity uplift and ensure coordinated responses to emerging risks.

[2] See section 8 of the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023*.