ABN 92 140 677 792
Property Exchange Australia Ltd

By online submission portal

16 September 2020

Re: Property Exchange Australia (PEXA) Ltd submission on the Department of Home Affairs consultation paper Protecting Critical infrastructure and Systems of National Significance

Attached is a submission from PEXA in response to the Protecting Critical Infrastructure and Systems of National Significance Consultation Paper.

Real property is critical infrastructure. As an Electronic Lodgement Network Operator (ELNO) PEXA is responsible for the facilitation of 75 per cent of land transactions nationally, and more than 95 per cent in NSW and Victoria. This places PEXA in a position to offer its experience in keeping Australia's largest asset class – the commercial and residential property market – safe and secure.

Real property transactions are critical to the functioning of Australia's financial system. Australia's land titling systems have been largely digitised over the past decade, in accordance with COAG's national electronic conveyancing reforms.

Central to this reform has been the introduction of the *Electronic Conveyancing National Law*, creating the legislative framework for the approval and regulation of ELNOs by the various jurisdictions.

Owing to the highly integrated nature of Australia's land titling system, which includes ELNOs, land registries, state revenue offices and financial institutions, a disruption in one part of the network can compromise the completion of transactions and the maintenance of records. Some $250 billion in real property is transferred annually, with residential property a store of more than $7.1 trillion of wealth.

PEXA proactively builds resilience against threats, including: new and evolving variants of ransomware that are becoming difficult to detect by typical signature-based antivirus solutions; avoidable misconfigurations in cloud and on-premises resources that allow attackers easy access to business systems; delays in patching critical flaws in operating systems and applications; credentials being stolen or cracked through weak or repeated passwords; and email phishing and business email compromise.

We build on our regulatory cyber security obligations to secure our Electronic Lodgement Network, as we continually seek to earn the trust of Australians to facilitate their most important transactions. PEXA's approach has been developed using input from ACSC guidelines, reviews of global data breach investigations and alignment to best-practice frameworks.

In its submission, PEXA recommends a set of priorities for combating cyber threats that if applied to the real property sector, would ensure Australia's regulation of critical infrastructure protects the most important asset most Australians will own in their lifetimes.

Regards,

Glenn King
Chief Executive Officer

ABN 92 140 677 792
Property Exchange Australia Ltd

Property Exchange Australia (PEXA) Ltd submission on the Department of Home Affairs consultation paper Protecting Critical infrastructure and Systems of National Significance

Who will the enhanced framework apply to?

1. **Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?**

In addition to those sectors identified in the consultation paper, land titling is worth examining by virtue of the fact that at $7.1 trillion, it's Australia's largest asset class, directly underpinning the wealth and economic prosperity of modern Australia.

Real property – compromising residential and commercial property – is a store of trillions of dollars of wealth. It represents the largest and most significant purchase many will ever make and remains critical to the functioning of Australia's financial system.

Underscoring all of this is the security of Australia's land titling systems, which have experienced accelerated digitisation over the past decade. This has been due to the successful fulfillment of COAG's national electronic conveyancing reforms, which represent one of the greatest examples of public-private cooperation in modern Australian history.

An estimated $250 billion worth of real property is transferred each year in Australia, with more than 75% of this now transacted electronically. In New South Wales and Victoria, this figure is now well in excess of 95%. To date, more than $1 trillion in property value has settled successfully online. At PEXA we are acutely aware of the instrumental role we play as custodian of Australia's largest property exchange and with close alignment to the banking system, the platform must be trusted, always on and reliable.

Critical to this reform has been the introduction of the *Electronic Conveyancing National Law* in most Australian states and territories, creating the legislative framework for the approval and regulation of Electronic Lodgement Network Operators (ELNOs) by the jurisdictions.

At PEXA we build on our cyber security regulatory obligations, seeking constantly to enhance our cyber capability and provide Australia with a trusted, safe way to transact property. We also seek to uplift cyber security across our immediate sector, continually educating our customers on cyber security risks and providing them with innovative solutions like our PEXA Key application, to reduce reliance on email for transmitting sensitive information. As the national economy begins to recover from the impacts of Covid-19, confidence in the security and reliability of systems that facilitate transactions and ownership will be even more crucial to supporting confidence in the property market.

ELNOs facilitate the preparation and completion of real property transactions through their integrations with state land registries (publicly and privately operated), state revenue offices, banks and financial settlement platforms (i.e. RBA's RITS). While ELNOs facilitate updates to title records, land registries are responsible for the maintenance of these records.

Due to the highly integrated nature of Australia's national electronic conveyancing and land titling system, a disruption in one part of the network can have adverse consequences to the completion of transactions and the maintenance of records.

2. Do you think the current definition of Critical Infrastructure is still fit for purpose?

Yes.

3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?

These factors are largely broad enough to cover relevant considerations.

While it may be implicit in considering the sensitivity of data and the well-being of individuals, given the increasing risks and therefore attention within the cyber sphere that is being directed to individuals' privacy, this dimension may be worthy of specific attention.

4. What are the common threats you routinely prepare for and those you have faced/ experienced as a business?

PEXA both internally as a business and within the broader property and conveyancing industry is proactively preparing for and building resilience against the following threats:

- New and evolving variants of ransomware that are becoming difficult to detect by typical signature-based antivirus solutions;
- Avoidable misconfigurations in both cloud and on-premises resources that allow attackers easy access to a business or business systems;
- Delays in patching critical flaws in operating systems and applications;
- Credentials being stolen or cracked, through weak or repeated passwords which in some areas includes sharing of credentials among users of a system; and
- Email phishing and business email compromise, which remains the most common entry vector for a cyber-attack. This is primarily due to continued reliance on email among our customers as a form of sharing sensitive information and the increased sophistication of email scams, which are in widespread use within the conveyancing sector to commit fraud against property transactions.

5. How should criticality be assessed to ensure the most important entities are covered by the framework?

The factors identified by the department in the consultation paper, including interdependency with other functions and consequence of a compromise should be the basis of assessing criticality.

An assessment that considers the magnitude of loss due to an infrastructure failure or breach event relative to others within a sector and across sectors will identify those that are most critical to Australian society and the economy. Dimensions for measuring loss should include human life and direct and indirect financial cost.

6. Which entities would you expect to be owners and operators of systems of national significance?

The openness of Australia's economy to trade and investment continues to play a vital role in building the prosperity that modern Australia enjoys.

We would expect the owners and operators of systems of national significance to be persons subject to Australian law, to ensure unambiguous compliance with regulatory requirements under the Act. This includes compliance with directions from the Government when responding to ongoing attacks.

While this needn't necessarily exclude persons who ordinarily reside or are incorporated in foreign jurisdictions from owning systems of national significance, the operations of these systems should be primarily conducted within Australia to ensure responsiveness to local conditions and the protection of Australia's data-sovereignty, and that Government agencies are capable of providing adequate assistance in response to significant cyber-attacks as has been outlined in the consultation paper.

Any person, natural or otherwise, that is subject to the laws of a foreign jurisdiction that may prevent their unambiguous compliance with the Act for whatever reason is likely to be an inappropriate owner and/or operator of a system of national significance.

Government-Critical Infrastructure collaboration to support uplift

7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?

Leadership and collaboration from the TISN are crucial for ongoing resilience in any sector. The level of leadership and subsequent action from a revised TISN should be symbiotic between Government, industry and even the public.

The ability to share intelligence on emerging threats or attacks that have been attempted or successful will enable organisations across similar sectors to adapt their own environments and controls effectively. This may require the removal of any stigma around the reporting of threats observed by individual organisations to encourage proactive intelligence sharing.

8. What might this new TISN model look like, and what entities should be included?

To date, organisations can align themselves to several different collaboration forums and standards. As the TISN model increasingly incorporates cyber issues into its focus, it should look to align to and provide centralised guidance from the Australian Cyber Security Centre (ACSC) and other competent agencies. In PEXA's case, the Australian Registrars' National Electronic Conveyancing Council (ARNECC) sets the standards. At the same time, regulators should provide the ability to easily map these to the ACSC or other requirements to enable prioritisation of controls to get the most value and protection for individual businesses or sectors.

It would also be advantageous to ensure that the TISN and ACSC are closely aligned, in the sense that membership of one can provide the benefits of the other. This would ensure less complexity in the number of sources of information organisations have for intelligence on cyber threats.

Members should include leaders across all the identified sectors, the ACSC and the Critical Infrastructure Centre to ensure an appropriate advisory board can be established. In addition, allowing advisors from leading security firms, especially in the cyber space, would be beneficial in providing the best quality guidance. This will assist in increasing the visibility of threats and standardising approaches to best practices being deployed by individual organisations.

9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?

Industries face many different regulatory requirements. These requirements can often overlap and complicate compliance for organisations while adding cost for no pragmatic cyber security benefit.

Ideally, the minimum compliance standards set for both Government and industry should measure against an agreed strategy such as the Australian Signals Directorate (ASD) Essential 8 to provide a baseline for cyber security. Guidelines could be established by the ACSC and TISN.

For example, by virtue of a significant proportion of PEXA's customers being financial institutions PEXA is in effect indirectly subject to obligations set by our customers' regulators, such as compliance with APRA's CPS 234 standard. APRA of course have no direct supervisory role over PEXA. Where cross sector dependencies like this exist, entities could operate and manage cyber risk with great ease and clarity if sector regulators set equivalent requirements that map back to national guidelines.

Positive Security Obligation

10. Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

The outcomes outlined provide a very high level and sensible approach that are relevant to all industries, whether they be critical infrastructure or otherwise. They convey the general message that organisations are responsible for understanding and managing their unique risk profiles, taking all reasonable steps to avoid incidents, building resilience into environments to withstand a potential incident and provide governance for continuous improvement.

11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

The obligations are sufficiently high level to apply to any industry. The detail and approach however will be up to each individual sector/organisation to scale based on their risk profile.

The obligations discuss the need for governance but in order to provide effective governance organisations need agreed frameworks against which to measure their effectiveness.

From our experience operating in a now largely digital sector, the National Institute of Technology (NIST) Cyber Security Framework and International Standards Organisation (ISO) 27001 standards have proven to be sufficiently broad in the sense that many businesses/organisations are leveraging them to both measure and prioritise the effectiveness of their Information Security Management Systems.

At PEXA we leverage the Secure Control Framework (SCF) which provides clear controls and outcomes across both these frameworks and other areas such as privacy to ensure we exceed any minimum standards laid out through regulation or otherwise.

12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

Most organisations dealing with critical infrastructure or sensitive public data are likely to already have risk management, reporting and other regulatory requirements that ensure these principles are applied in one form or another. There is the chance of a clash depending on which best practice framework each organisation has chosen and the sector specific standards that a designated regulator adopts.

In critical infrastructure sectors with a high degree of exposure to cyber risks, ensuring the sector's designated regulator considers the suitability of allowing regulated entities to align with existing frameworks like the ACSC's may reduce unnecessary regulatory burden.

13. What costs would organisations take on to meet these new obligations?

In the unusual event of an operator of critical infrastructure or a system of national significance not having an established risk management and security function, the initial investment would be challenging – especially in terms of setting up new teams, performing assessments and deploying new controls to meet obligations.

If an organisation in one of the identified sectors did not already have even an entry-level capability in this space, the cost would be readily justifiable against the potential consequences of inaction.

14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

It is reasonable to believe that several of the sectors identified would already face these obligations in some form, especially finance or utility providers where a potential incident can result in economic collapse or loss of human life.

Organisations' costs regarding these obligations are typically commensurate to their unique risk profiles. However, costs are generally incurred as a direct result of auditing and compliance requirements, human resources, and technology to implement appropriate controls.

While the obligations certainly provide the right mindset for organisations to adopt, it is important that proposed regulatory or policy changes that have ramifications for cyber security and associated risks are develop by or with appropriately skilled experts. This could be achieved through enhancing the cyber capabilities of regulators or through ensuring that greater consultation with industry and cyber security experts is carried out. It is possible that, in some instances, increases in cyber-risk are inaccurately weighed, resulting in potential unintended consequences. In many cases, regulation and regulators are not equipped to understanding the cyber implications of their decisions. This appears to be an increasing issue across governments and regulators.

Regulators

15. Would the proposed regulatory model avoid duplication with existing oversight requirements?

The proposed regulatory model for implementing the Positive Security Obligation (PSO) would, in theory, avoid duplication with existing oversight requirements, through empowering existing regulators under the Act to baseline existing requirements and extend upon them as required to meet the principles-based outcomes and security obligations described.

Critical to the success of this approach will be to ensure that all designated regulators, whether they administer existing powers under Commonwealth or state and territory legislation, are appropriately skilled and resourced to administer powers under the Act. It is envisaged that in some circumstances, an uplift in capacity and/or capability could be required as well as additional funding.

16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?

General guidance on the areas of obligation that are of relevance to the industry in question should be developed in close consultation with industry stakeholders. This will allow each sector to focus required resources in the areas that provide the best return on value from a cyber perspective and ensure ongoing governance.

Building a standardised reporting regime into ongoing governance with the sector regulator would aid in providing focus and ongoing improvement against obligation requirements. However, this reporting should be closely aligned to the security obligations and any chosen frameworks used to monitor/measure the organisation's control environment.

17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

In relation to land titling, the Registrar of Titles in each state and territory jurisdiction as a member of the unincorporated Australian Registrars' National Electronic Conveyancing Council (ARNECC) is responsible for –

a. The regulation of ELNOs including issuing Approvals to operate and the Operating Requirements; and
b. Operating, or regulating the private operation of, the land registries.

Given Registrars have an intimate understanding of the land titling system within their jurisdiction, they have been best placed to regulate ELNOs and private land registry operators to date.

The Operating Requirements currently place cyber security obligations on ELNOs which include extensive requirements to develop, implement and keep current an Information Security Management System and to otherwise secure the Electronic Lodgement Network. Accompanying these requirements are reporting obligations that range from immediate notification in the event a transaction is jeopardised through to monthly and annual reporting on the performance of IT systems and risk management frameworks.

While we believe that existing requirements for ELNOs are comprehensive enough to meet the cyber security threats we face, we note that ARNECC and the Registrars are heavily reliant on independent experts to review and attest that frameworks developed by ELNOs are fit for purpose.

We believe that when it comes to cyber security issues, ARNECC is not fit for purpose to meet the national cyber security environment that ELNOs face, so far as its current disparate state-based form and capabilities are concerned. As our market has evolved and Australia's cyber risk profile has increased, the lack of clarity around the role of the states in regulating cyber security issues in a national sector have become more pronounced.

Ensuring sector regulators are capable of administering the Positive Security Obligation as is envisaged by the Department will be important to the success of this reform, ultimately measured in the trust that Australians have in the management of critical infrastructure by governments and entities.

18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

As highlighted above, clear guidance for sector regulators on capability requirements to effectively monitor and enforce the Positive Security Obligation would help to ensure there is a baseline competency across the regulation of sectors under the Act.

Given the increasingly dynamic pace at which threats and issues evolve while managing cyber risks, sector regulators need to be involved beyond licencing and overseeing conduct and prudential matters. As appropriate, they should also be responsible for establishing guidance on and policing industry issues around technology resiliency, adherence to minimum standards and the establishment of appropriate market entry criteria.

A dynamic cyber security operating environment and risk profile requires a regulator with the capability to respond to issues when and as they arise with industry.

19. How can Government better support critical infrastructure entities in managing their security risks?

As per response to question 9, simplifying regulatory and compliance environments will play a significant role in enabling organisations to focus on uplifting their control environments to better manage risks. Similarly, it would be advisable to provide centralised and agreed control frameworks against which organisations can align. Potentially leveraging existing recognised best practice frameworks, for example ASD Essential 8, NIST, ISO 27001 or higher, depending on the sector risk profile.

20. In the AusCheck scheme, potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?

Under the Operating Requirements to which ELNOs are subject, good corporate character and reputation requirements extend to the taking of reasonable steps to ensure that employees, agents and contractors are not and have not been subject to various matters. These include insolvency events, convictions for fraud and other offences in connection with business and commercial activities and other professional disciplinary events.

Given the increasing threat environment that many operators of critical infrastructure face, the AusCheck scheme or a similar model would be useful in ensuring a more comprehensive set of checks are carried out to address insider threats.

We are unaware as to whether the operators of other critical systems in our sector, including land registries, are subject to similar character check obligations.

21. Do you have any other comments you would like to make regarding the PSO?

No.

<u>Enhanced Cyber Security Obligations</u>

22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

A zero tolerance for cyber risk is a cornerstone of PEXA's strategy. PEXA’s approach has been developed using input from ACSC guidelines, reviews of global data breach investigations and alignment to best practice frameworks. As such PEXA's recommendation for prioritisation to combat current threats should ideally focus on:

- Alignment to at least one essential cyber security control framework;
- In-depth controls for ransomware such as Application Whitelisting and protective controls on emails and web browsers;
- Multi-Factor Authentication (MFA) as a non-negotiable on any service or application available on the internet;

- Continuous vulnerability management set via strict targets for patching and then ongoing measurement to ensure objectives are met;
- Clearly defined network policies and service configurations outlining what is required for the business, including the removal of access to anything that is not;
- Monitoring of all network activity;
- Control the damage that can be done through stolen accounts by ensuring all access is limited to precisely what is needed to perform users' required duties;
- Clear guidance for operators on managing user risks for their own staff and as appropriate their customers, such as recommending zero-tolerance for use of vulnerable channels like email for the transmission of sensitive information (i.e. banking details or credentials); and
- Ongoing security awareness and training through email phishing tests, education sessions and communications.

23. What information would you like to see shared with critical infrastructure by Government? What benefits would you expect from greater sharing?

When it comes to emerging threats, the more information an organisation's Cyber Team can receive in a timely fashion, the better.

This primarily includes details of any new threats that have already been used to attack or compromise an organisation. This would ideally be in the form of indicators of compromise (IOCs) that organisations can ingest into their existing security tools or Security Operations Centre (SOC) monitoring, so that an organisation can determine whether it is at risk, how to best mitigate and if it has already been compromised.

24. What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?

At PEXA we have a dedicated SOC team that monitors our core platform, customer account activity, corporate environment and integrated third parties for suspicious activity.

Most organisations with this type of functionality would ideally be able to contribute details of attempted, mitigated and sometimes successful attacks, including details of the attacker's tactics, techniques, and procedures (TTP) to help identify IOCs that can shared amongst the broader community.

With fraud playing a key role in the risk profile to the industry which PEXA serves, the ability to share detail of scams observed within our network could also be provided to further enhance TTP information in this space.

25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

As with scanning an internal environment for vulnerabilities, external scans against the perimeter of a network or any other public facing infrastructure is essential. There should be a zero tolerance for any identified vulnerabilities in this space.

Organisations should know all the ingress and egress points within their network and ensure they have appropriate traffic inspections engines setup at each point. This can include signature-based intrusion prevention systems (IPS) and ideally machine learning capabilities with threat intelligence feeds to analyse traffic for anomalies or other IOCs.

26. What are the barriers to owners and operators acting on information alerts from Government?

A major barrier is the timeliness and format in which that information is received. As previously stated, organisations need to receive IOCs or other intelligence quickly when new threats are emerging in a method that can be easily ingested to sweep the environment for any risk.

27. **What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?**

Any playbooks developed by the Government and industry should be based on a principle that intervention by the Government is a last resort in the most extreme of situations.

One of the challenges that occurs in creating playbooks within organisations is in determining the most effective set of playbooks that warrant priority. It is easy to look at the history of incidents and fixate on the most commonly occurring event types, as these are most in need of reproduceable steps for consistent response. Generally, these are also the lowest-impact events, such as broad phishing or general malware. In cooperation with Government and wider industry, there is a need for a standard set of playbooks that are determined based on the prevalence of an attack globally as well as potential impact. Ideally an open standard would be available for formatting, so that these playbooks could be used in Orchestration and Automation tooling platforms with little customisation.

Potential challenges in co-developing playbooks include scenarios which might unwittingly disclose confidential information about internal processes to competitors or detractors, although this is an issue that is regularly and successfully addressed by technology professionals. Perhaps a greater barrier exists in determining a uniform format that does not require or preclude any particular technologies or controls. One of the reasons this problem has not yet been solved by private industry is the fact that there is no “one-size-fits-all” approach to creating playbooks, and each organisation would require extensive tailoring of any solution.

Ideally, it would be useful to have industry and/or government templates for a broad range of scenarios, perhaps tied to the MITRE ATT&CK Framework or similar widely-adopted map of intrusion techniques and tactics, that could be used directly as a blueprint within common Security Orchestration and Automation, and Response solutions. With an open standard, organisations could contribute customised playbooks back into an ecosystem that fostered actionable and universal response actions.

28. What safeguards or assurances would you expect to see for information provided to Government?

It is reasonable to expect that organisations will only provide Government with specific TTP information over anything operationally sensitive or proprietary, depending on the situation. Typical safeguards

around data handling would indicate that Government would be upholding the same obligations as industry.

In terms of assurances, PEXA would like to see any information provided to Government turned into regular and actionable intelligence for the broader landscape of critical infrastructure providers within Australia.

Cyber Assistance for entities

29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

It would be beneficial to understand in greater detail the types of activities that the Government currently believes could form part of this type of intervention. PEXA's initial position on the limited information available is that there are three scenarios where direct action may be requested or required.

- Where an individual organisation or sector request direct action assistance from the Government in the form of dedicated incident responders where containment and recovery efforts are taking longer than would be desired. This would be dependent on the sector involved and the impact of the incident.
- Where an incident or attack has crossed a threshold where the impact on the economy, national security or public health/safety is severe and the Government has substantial grounds to believe that the impacted entity is not taking steps to respond to the attack in a timely manner in accordance with Australia's national interest.
- In extraordinary situations when the impact of a severe attack spans multiple organisations and/or critical infrastructure sectors and the Government has establishes that it is the only actor able to coordinate containment and recovery efforts effectively.

Further engagement with impacted sectors to define the parameters of powers under consideration is necessary. This engagement could be managed through or with existing forums such as TISN, ACSC and even ASD.

30. Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?

Any thresholds and responsibilities should be agreed to in consultation with sectors. Given the uniquely holistic view that the Commonwealth has within the Australian context and the breadth of the powers under consideration in the consultation paper, the Minister for Home Affairs is the appropriate person to declare such an emergency and to authorise subsequent direct action, subject to appropriate limitations.

Similar to the existing regime under the Act restricting the Minister's ability to issue directions, a government agency with appropriate capabilities should be required to issue an independent assessment that confirms there is an ongoing emergency that meets the parameters set in the Act. The Minister should also be required to consult with impacted organisations prior to a making a declaration.

31. Who should oversee the Government's use of these powers?

We understand that the Government's use of the existing powers to issue directions under the Act are subject to judicial review. We would anticipate that the Government's use of powers under the amended Act, including to issue directions and to declare an emergency would continue to be expressly subject to judicial review.

Furthermore, embedding in the amended Act a set date for a future review by the Parliamentary Joint Committee on Intelligence and Security would provide industry with confidence that this reform is being given appropriate parliamentary oversight. A review could assess among other things the effectiveness and proportionality of the Government's use of powers under the Act.

Given the potential imposition powers under the Act may have on the operations of private entities and the importance of our collective success in protecting the essential services that all Australians rely upon, referral to the Joint Committee would provide an appropriate, arm's length forum for review.

32. If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?

We believe it is appropriate for Government to determine what actions it should take to disrupt attackers, given the unique view Government has owing to its intelligence capability, responsibilities for Australia's defence and foreign affairs and the complexities presented by responding to state and non-state actors.

33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?

Without more detailed information on the types of actions that Government may consider taking during an emergency, and that industry could be directed to take, a comprehensive response to this question is not possible.

As a starting point however, given the significance of the powers and associated responsibilities that the Government are considering for themselves in this reform, protections should be appropriately limited so as to not incentivise Government now and into the future to take actions that would cause harm or loss that is disproportionate to the benefit derived from their action.

In relation to industry, protection from liability for entities and their officers should apply when following directions of Government. Furthermore, legal protection should be provided when decisions are made in good faith and in reliance on information and advice from experts, that an entities officers reasonably believe to be competent and qualified.

34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?

Existing safeguards in the Act should be built upon to make them fit for purpose under the amended regime.

The Minister should not be able to issue a directive or declare an emergency unless –

- A Government agency (whether that be ASIO or in the cyber context the ASD/ACSC) issues an adverse security assessment or equivalent;
- Good faith engagement with the operator or owners of impacted critical infrastructure has occurred; and
- The Minister has assessed that the direction or direct action in an emergency is proportionate to the risk, including considering costs incurred by the entity.

35. What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?

Given the proposed extension of the Act to elevate the Government's ability to respond to cyber attacks through the issuing of time-sensitive directions and to take direct action following the declaration of an emergency, it is difficult without precedent or further information on the proposed powers to fully anticipate the costs and risks to industry.

36. Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?

The obligations/assistance mix may need further clarification as per PEXA's previous responses. Organisations would need to take potential government assistance/intervention into consideration as an impact or outcome of a potential risk event. This could trigger a reevaluation of current risk registers and treatment plans as an organisation may look to avoid government intervention.

For some organisations having a third party such as the Government intervene could be viewed as a high visibility or impact event and current managed risks would need to be revaluated with that in mind. Additionally, organisations would need to consider how to share information with the Government, systems access and how roles and responsibilities would change based on the level of assistance being provided.