14 April 2023

Australian Government
Department of Home Affairs
Expert Advisory Board appointed by Minister for Cyber Security
Belconnen ACT 2600

Delivered by webform to: auscyberstrategy@homeaffairs.gov.au

Dear Advisory Board,

Loan Market Group welcomes the opportunity to provide a submission in response to the 2023 - 2030 Australian Cyber Security Strategy Discussion Paper released by the Minister for Cyber Security's office.

We believe in a strong and cyber safe digital economy, not only for the businesses offering the products and services, but also to ensure the cyber safety of Australian consumers. You will find our submission to the Discussion Paper's questions in the Appendix that follows.

About Loan Market Group

Loan Market Group (The Group) is a family-owned business and has, over 29 years, grown to be what is now considered Australasia's biggest aggregator. The Group offers services and support to over 5000 mortgage and finance brokers (credit assistance providers) across Australia, approximately half of which are authorised representatives of one of The Group's three (3) Australian Credit Licences (ACL). The remaining broker businesses represent individual small businesses who hold their own respective ACL.

The Group's network of brokers have helped over 1,000,000 Australian customers. A large and growing number of Australians are choosing the services of a mortgage broker. The latest report[1] by the Mortgage and Finance Association of Australia (MFAA) identifies nearly 70% of mortgages written in Australia between October and December 2022 were facilitated by brokers.

[1] Source: MFAA's quarterly survey of leading mortgage brokers and aggregators October - December 2022, (https://www.mfaa.com.au/news/mortgage-broker-market-share-reaches-new-december-quarter-record

We thank you for the opportunity to provide this submission. If you have any questions or require any further information, please do not hesitate to contact me on either [redacted] or by email to [redacted].

Kind regards,

[redacted]

Stefania Riotto
Head of Broker Regulation & Policy, Loan Market Group
Level 26, 135 King Street, Sydney NSW 2000

APPENDIX

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?	We would like to see the strategy include the following: ● Moving security higher up in the supply chain - the tech giants (such as Microsoft, Apple, Google) who deliver the operating systems our computers use and the major internet providers that deliver the cyber world to businesses and citizens alike (Telstra, Optus, TPG and the like) need to focus on stronger built-in protections for operating systems, internet traffic and devices. ○ It is inefficient to have every small business or individual trying to protect themselves. ○ It would improve the speed at which an IP address, if found to be a bad apple, can be automatically blocked by all operating systems. We shouldn't have to wait for something to happen on Australian soil. ● Incentives for reporting events that disrupt a business' operations. Reporting is useful but if it is onerous or will result in small business bearing additional (investigations) costs, it will discourage participation in the reporting regime especially given the resources required by regulators to police such a regime. ● A focus on promoting cyber security education and awareness with both small business and the general public to help reduce the vulnerabilities to cyber threats. ● A mechanism for international cooperation to punish the holders of data similar to the way Anti Money Laundering and Counter Terrorism Funding has international components to ensure compliance with the regime.

2. What legislative or regulatory reforms should Government pursue to:enhance cyber resilience across the digital economy? **a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?** **b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?**	A. Regulate to ensure that all businesses are required to follow ACSC guidelines and to have and to test, confirm and publish that the following three items are in place: - Business Continuity: The ability to restore all of the data from a safe backup - Access Controls: That proper multi-factor authentication (or password-less such as face ID) is set up on all access points - Incident Response - The ability to get their business back up and running again With penalties in place for organisational failure. However, there needs to be careful consideration of the impact to small business, any new obligations should be proportionate and scalable to business size and extensive compliance support (including subsidisation support) to small businesses must be provided before any new obligations commence. Please see further feedback captured for Question 15. B. Yes, we believe in further reform to the Security of Critical Infrastructure Act to extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in the definition. All infrastructure is critical - a laptop used by a small business is a critical asset to that small business. Consideration however should be had to make sure that the implementation is economically possible for all types of business.

c. Should the obligations of company directors specifically address cyber security risks and consequences?	C. Yes, we agree that directors need to be looking at any threat to their company's existence, and cyber today is one of the main threats. It is important that the Strategy support, not replicate, work already undertaken to address director's obligations, for example by the Australian Institute of Company Directors which have established the Cyber Security Governance Principles for company directors: 1. Clear roles and responsibilities 2. Develop, implement and evolve a comprehensive cyber strategy 3. Embed cyber security in existing risk management practices 4. Promote a culture of cyber resilience 5. Plan for a significant cyber security incident
d. Should Australia consider a Cyber Security Act, and what should this include? **e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?**	D & E. Yes, we support Australia considering a Cyber Security Act, as well as a Minister with responsibility for it. The Act should be a consolidation and simplification of all the different regulations and legislation that exists today (such as the Privacy Act, APRA's CPS 234, and other regulations and legislation that focus on risk, and business continuity). The Act's main consideration is to protect private information, and ideally would align to international standards. The discussion paper already acknowledges that the development of the Strategy will be in parallel with a number of reviews, including that of the Attorney-General Department's Review of the Privacy Act 1988. We see this as a welcome opportunity to simplify the complexity of data retention requirements. Having simpler rules means it will be easier to regulate.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: **(a) victims of cybercrime; and/or** **(b) insurers? If so, under what circumstances?** **i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?**	F. We believe the Government should not prohibit the payment of ransoms. If it's the difference between the business failing and having a reasonable chance of continuing - we believe it should be a business decision to make. Generally speaking, there are 2 situation in which ransoms could be sought: ● A cyber attack poses both a reputational disaster and potential disaster for impacted customers. Paying ransom potentially doesn't just protect the business, it could protect the customers whose data is compromised from being publicised. ● The other instance is when a hacker encrypts data on a device and then seeks a ransom in order to get a "key" to un-encrypt the device. This is an avoidable situation if the proper data backups and incident response plans are in place. As part of obtaining cyber insurance for a business, the insurers generally check and review the business, its policies and processes, before providing the insurance cover. In a way, the insurer acts as an assurance function for a business and that they've taken reasonable steps to protect their business.
g. Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?	G. Yes, the Government should clarify its position, however it should not legislate a ban on the payment of ransoms (refer response to question F.) We suggest there be a middle ground... payments is what allows the "bad apples" to stay in business. If no-one paid then there's not an industry or at least only the market for sale of ill-gotten data. Having said that, we believe penalties here should be civil rather than criminal and the criminal penalties need to apply in the last part of the market, i.e., to those buying the data. Criminal penalties and lengthy incarceration time should be associated with obtaining and/or being in receipt of stolen data.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?	Australia should take the lead in this area as it is well-placed to be a provider of intelligence and information sharing to improve the security of our neighbours.
4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?	Australia has the opportunity to work with its existing defence network. Cyber resilience is a defence initiative. Cyber attacks occur mainly in the more developed nations of the world, so there is opportunity to elevate international conversations with existing partners (such as the US, UK, Europe) to include mechanisms for deliberate capture and sharing of cyber intelligence. Australia should not try to be independent in its cyber protections.
5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?	The laws and standards set a benchmark for businesses and individuals for law abiding countries - this is OK, but there will always be bad apples. Consideration for a *Global Cyber Intelligence Exchange* is required so that when a cyber attack occurs anywhere in the world, it would be reported to the Exchange and the details of the attack shared instantly with all participating members, so that other nations (businesses) can prepare and block a potential attack on them. There are four (4) main operating platforms on technology used by individuals and businesses (ie., Windows, Google, Linux and Apple). There is an opportunity to employ the strongest technical minds at the highest level - if these operating platforms were monitoring what was happening on people's devices and inputting details of cyber threats into a Global Cyber Intelligence Exchange, then everyone else should know to block that threat and can do so proactively rather than reactively.

	Another aspect is to leverage the connections Australian regulators (such as APRA, ACCC and ASIC) have with their global counterparts. What work is already underway in particular to understand and set standards and regulatory framework for the digital financial system (digital currencies and assets) to which Australia can contribute and/or lead?
6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?	Apart from establishing a Cyber Security Act as noted earlier (refer to question 2D), government can take a lead in demonstrating best practice - for example: ● Have all government departments operating to ISO 27001 or the SOC 2 Type II standards if not already doing so, and ● that in the procurement practice - that all supply chains involved with government departments are also operating to the same standards.
7. What can government do to improve information sharing with industry on cyber threats?	Military, civilian security forces, police intelligence services, the Australian Federal Policy, and the like, are all intelligence services trying to understand and tap into criminal activity. If information is captured and put into a usable form such as via a 'cyber intelligence exchange' mechanism, the learnings from that intelligence can be shared with industry more broadly.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?	Yes. The prime concern is the protection of the compromised individuals' data. Our view is • The prime goal is to fix the problem - and businesses will want all the assistance (and specialists) possible without regard to consequences to help resolve the issue. • Once the issue is resolved, to have the breached organisation advise (the cause and remediation) to the regulators through the existing reporting mechanisms already in place for those organisations. For example through the notifiable data breaches regime. The regulators should have confidence in the ACSC and the ASD to provide the breached organisation the required assistance to resolve any attack. Further, confidentiality will provide breached entities with the ability to manage the messaging to the rest of the market and subsequently be more likely to seek assistance if it is clear that the entity will not immediately be named and shamed.
9. Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?	It would only improve the public understanding of the nature and scale of the cybercrime if the results and insights of the data collected is published and shared with the public in ways that the public will be able to see and understand it. Need to describe the results of data in common language for the public to be able to understand For example - the Office of the Australian Information Commissioner (OAIC) publishes data on notifiable data breaches[2] - but how it gets shared more broadly with the public needs consideration. Those who want to know the information can go directly to the OAIC website, but for the average Australian, they won't know to do this.

[2] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2022

10. What best practice models are available for automated threat-blocking at scale?	With the presumed goal in mind for the model to aggregate cyber intelligence and provide real-time distribution to all parties involved in protecting against cyber crime, there is currently a Cyber Threat Alliance that should be considered as best practice and expanded to be on a more global scale. The Cyber Threat Alliance (www.cyberthreatalliance.org), based in Arlington Virginia in the United States, is a non-profit organisation that is working to improve the cyber security of the global digital ecosystem by enabling real-time, high-quality cyber threat information among companies and organisations in the cybersecurity field (currently it has 36 private-sector members). An option to consider is regulation to mandate that technology providers hold membership in this (or this type) of alliance.
11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?	Yes, Australia requires a tailored approach to uplifting cyber skills beyond the broader STEM agenda. There needs to be cyber security education to support the proposed Cyber Security Act. Australia should be making sure that it has sovereign capability in cyber security, much like it has approached its defence with the AUKUS agreement (which aims to strengthen Australia's national security and contribute to regional stability and to build a future made in Australia, by Australians, with record investments in defence, skills, jobs and infrastructure[3]). To that end, we believe it necessary for a review of the secondary school curriculum and expansion for topics like cyber security to be required subjects.

[3] Prime Minister of Australia Media Release 14 March 2023, https://www.pm.gov.au/media/aukus-nuclear-powered-submarine-pathway#:~:text=The%20agreement%20will%3A,%2C%20skills%2C%20jobs%20and%20infrastructure.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?	With regards to education - our feedback remains as for question 11. With regards to accreditation - yes, there is a need for broader accreditation and recognition of cyber skills and specialities. Much like electricians and builders are licensed, so too should those we rely on for our cyber security. Accreditation should not matter for immigrant or local skill, provided the process is robust and sufficient to identify the authenticity of the individual and their skill and capability. There are a lot of people offering advice on cyber security but how can we be certain of their training? There is a need for formal cyber training to be recognized to build resilience and trust in the system. Training should be based around International Standards and minimum ongoing professional development requirements.
13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians? **a. Should the government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?**	Yes, we support the government considering a single reporting portal for all cyber incidents. Simplifying the reporting process will provide efficiencies and improve compliance with the regime. We note however, when considering the feedback to this question that it also takes into account the feedback to question 8.

14. What would an effective post-incident review and consequence management model with industry involve?	Effective models are clear on what is being reviewed, keeps the critique constructive, is factual and objective and prepared in a timely manner. In addition, there are two components we believe are key to consider for the model - ● Asking the independent specialists involved in the resolution of the incident to prepare an objective third-party post-incident review. ● Sharing that report with industry associations for them to share the learnings with membership more broadly. In this way, the objectivity of the report can be reviewed and challenged (similar to a peer-review process). If one knows that it will be made public, then the report will need to be objective and fair.
15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime? **a. What assistance do small businesses need from the government to manage their cyber security risks to keep their data and their customers' data safe?**	Small businesses accounted for over 97 per cent of the 2.6 million Australian businesses in 2021-22. In 2020-21, they employed over 5 million people and generated around a third of private sector output, a $438 billion economic contribution.[4] The Australian Bureau of Statistics (ABS) Business Conditions and Sentiments Survey (June 2022) found almost a third of employing businesses were having trouble finding staff, were facing increased operating expenses, and more than 2 in 5 (41 per cent) were experiencing supply chain disruptions.[5] With that context, it is important for government to have a coordinated effort to address the issues faced by small businesses.

[4] ABS (2022) Counts of Australian Businesses, including Entries and Exits, July 2018-June 2022, released 25 August; ABS (2022) Australian Industry, 2020-21 financial year, released 27 May
[5] ABS (2022), Business Conditions and Sentiments: Insights into Australian business conditions and sentiments, June 2022

	When it comes to customer data and personal information and its safety - government should review and remove practices and regulations that ● place obligations on holding personal information, and ● improve the required removal and deletion of information after a person has been identified. ● Explore alternative methods of identification of individuals so that personal information is not required to be held. We need government and industry to be ruthless and remove the need to retain personal data once its original purpose has been served. For Loan Market Group, we are in an industry that is already highly regulated - with multiple requirements from different Acts - to collect and retain personal and sensitive information for various lengths of time. We welcomed the opportunity to contribute a submission to the Privacy Act Review Report (the Review) consultation by the Attorney General's Department in March this year. The Review's Proposal 21.6 will undoubtedly illustrate the complexity of navigating data retention requirements across multiple legal requirements - aligning, or ensuring the intended policy objectives of each are met with reduced complexity is welcomed. We acknowledge too, that the Review proposes to remove the small business exemption. Any new obligations should be scalable and proportionate to business size. Careful consideration and consultation with small businesses is a must. So is the consideration of feedback from victims of cyber crime and their real-life experiences as it will likely identify a number of areas where small businesses will need support to improve their cyber security posture. When it comes to cyber security risks and helping small businesses

	to manage these - a key aspect is to help make it easier to get cyber security insurance. Insights (and then changes to improve) can be derived from knowing why and when a business doesn't qualify for a policy - using that knowledge to improve the overall process and ability for more and more small businesses to obtain it.
16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?	Encourage the big technology companies to work together - for example, when purchasing a computer, the user then has to install an operating system, and then install a virus protection tool, and potentially other separate tools to enhance security and usability. Why can't it all come together? The key message is to build it safe from the start, and not have to rely on the individual user to complete the added steps to make the tool safe.
17. How should we approach future proofing for cyber security technologies out to 2030?	Refer to our response to Question 1. Further, with regards to new and emerging technologies, it is incumbent on the producer that ethical responsibility also applies.
18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?	Yes. Government has the opportunity to ● only buy from providers that produce cyber secure versions of the products. ● only allow the import and sale of technology products (Hardware & Software) that have been produced and certified to be cyber secure and resilient. ● Government should be utilising its own procurement functions to ensure that it is only purchasing from entities that have and maintain a minimum standard of cybersecurity i.e. ISO 27001.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?	Consider legislating that emerging technologies should have cyber security by design incorporated into those technologies.
20. How should government measure its impact in uplifting national cyber resilience?	Key measures to consider are: ● The number of successful attacks per head of population (per 1 million people) compared to the G7 average ● The number of records exposed and the number of business days lost
21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?	Transparency will be supported by publishing the data noted captured by Question 20, including any applicable trend lines. We would also encourage government to schedule a 3-year review to see how the implementation of the strategy is progressing.