National Australia Bank
395 Bourke Street
Melbourne VIC 3000

14 April 2023

Andrew Penn AO
Chair, Expert Advisory Council
Australian Cyber Security Strategy (2023-2030)

By email: auscyberstrategy@homeaffairs.gov.au

Dear Mr Penn,

NAB Submission on the Australian Cyber Security Strategy (2023-2030) Discussion Paper

National Australia Bank Ltd (NAB) welcomes the opportunity to provide a submission to the Expert Advisory Board on the *Australian Cyber Security Strategy 2023-2030*.

NAB is committed to contributing on this issue as evidenced by regular engagements with Government and its agencies, through formal feedback on previous strategies (2016 and 2020) and most recently, feedback on the *Security of Critical Infrastructure (SOCI) Act*.

NAB supports the intention to improve the legal and policy frameworks critical to effective cyber security. This submission focuses on five key areas which NAB believes are critical to keep banking, and other, customers across the nation safe:

1. Mandated cross-sector approach
2. Clear and streamlined regulation
3. Supportive government-industry frameworks
4. Boosting community awareness and education
5. Developing cyber skills

In this regard, NAB has chosen to respond to a select number of the 21 questions contained in the Cyber Security Strategy Discussion Paper, of most relevance. NAB has also contributed to the submission provided by the Australian Banking Association (ABA), of which it is a member.

Background

Cyber security in Australia has a strong foundation on which to build. While NAB is motivated to see and contribute to ongoing improvement, it is important to ensure the current system is enhanced without removing valuable assets and processes already developed. The roll-out of the national Cyber Threat Intelligence Sharing (CTIS) platform, stronger cyber leadership from Government, greater corporate investment, and the updated *Critical Infrastructure Act*, exemplify progress made to date.

NAB notes the forthcoming changes to Australia's digital landscape which continue at pace. The impact of changes out of the Privacy Act Reform Report and progress on the Consumer Data Right regime and Trusted Digital Identity Framework (TDIF), are notable. NAB encourages Government to consider these, and other, reforms alongside any variation to cyber security requirements. Together they represent a significant

©National Australia Bank Limited ABN 12 004 044 937 AFSL and Australian Credit Licence 230686

opportunity and suite of regulatory reforms which should be implemented harmoniously and will require careful sequencing to enable effective delivery.

As Australia's largest business bank, and advocate for our business customers, a uniform regime that clearly communicates the obligations on business is critical to successful compliance. As noted in feedback to concurrent reviews such as the *Privacy Act* consultation, NAB supports the creation of a clear reform roadmap, that is mindful of all business' capacity and capability to comply. This should also have regard to bottlenecks in Australia – for instance the serious shortfall in cyber security expertise, which is also addressed later in this paper. The standards set for industry must also be modelled by Government who hold some of the country's most sensitive data and systems.

Customer trust and confidence is central to NAB's mission to serve customers well. Strong cyber security is central to building and maintaining that trust and confidence. Over the past few years, we've seen the single largest transformation in banking in Australia's history as more people choose to bank digitally. More than 93% of NAB customer transactions now take place online[1]. The digital transformation of the global economy means the way people learn, shop and work will continue to evolve, and it is incumbent on Governments, with industry, to provide a safe and secure transition.

1. Cross sector approach

Question 2: What legislative or regulatory reforms should Government pursue to enhance cyber resilience across the digital economy?

Building a resilient economy in the digital age, with a thriving cyber ecosystem at its centre, can only be achieved through strong and consistent partnerships between governments, business and consumers.

NAB has established strategic intelligence and capability sharing partnerships with the Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC) and the Australian Signals Directorate (ASD). Additionally, we have seconded staff to the AFP and have similar plans with the ASD's Australian Cyber Security Centre (ACSC). NAB remains steadfast in its willingness to partner with Government, and other organisations, to create a safer Australia for our customers.

While large organisations such as NAB have the capability and resources to install robust cyber security defences, many smaller businesses have limited ability to protect themselves and their customers. This reinforces the need for a strong whole-of-economy approach to strengthening Australia's cyber defences.

Where necessary, NAB encourages Government to mandate the involvement of specific sectors if required to ensure this whole-of-economy approach. This is a moment for Government to ensure Australian businesses adopt a consistent national framework that does not discriminate based on a person's internet supplier or whether they bank with a small or large provider.

CTIS

An example of where NAB believes this could add value is to strongly encourage participation in the Cyber Threat Intelligence Sharing (CTIS) platform. NAB was the first organisation to use the CTIS platform and has shared intelligence via CTIS, including threats targeting other Australian organisations. It is a strong example of the value of cross sector collaboration. The value of this platform would be greater if more large organisations were involved.

[1] NAB News: An update on how we're reshaping our branch network

©National Australia Bank Limited

Clean Pipes
NAB would welcome further Government work with the telecommunications and other sectors on a mandated Clean Pipes program, designed to ensure the country's internet traffic is cleansed from known-malicious activity. This kind of program, using various technologies to provide default security to clients, would provide benefits across the economy and for all Australians.

While these capabilities are being used in various ways around the world, they are not automatic and often come at an additional price to consumers. As outlined in this paper, education, awareness, and skills development are critical but must complement a robust prevention program.

The ASD and ACSC are making positive inroads to combatting the threat environment. The private sector must be encouraged, and where necessary mandated, to play its role in supporting the Government by sharing intelligence and working together to combat malicious actors. Enhancing this capability could require changes to privacy provisions in the *Telecommunications Act*, which should be pursued.

Minimum Cyber Security Standards
Additionally, NAB recommends Government adopt minimum cyber security standards for Software as a Service (SaaS), cloud storage and IT service providers doing business in Australia and storing or processing personal information (IT Providers).

Australian business, and particularly small to medium enterprises, are heavily (and increasingly) reliant on such providers to maintain the security of their systems and their customers' data. These businesses typically contract on standard form contracts with IT Providers on a 'take it or leave it' basis. These standard-form contracts are generally designed to minimise the IT Provider's responsibility and liability for cyber security, which reduces incentive to invest in and prioritise robust cyber security.

To address this, we recommend that IT Providers are subject to additional specific regulations in relation to cyber security which do not rely on bilateral negotiations between IT providers and their customers.

One way of legislating this would be to leverage the existing obligation in Australian Privacy Principle 11 (*APP11*) to take '*such steps as are reasonable in the circumstances to protect the information*' and amend it to further define the most important steps that are required to discharge that obligation.

To do this APP11 could be amended to reference a new statutory regulation based on ACSC's 'Essential 8'. If the steps referred to in the new regulation have not been taken, and this enables a cyber security breach, there would then be a rebuttable presumption that the obligation in APP11 has not been discharged by the IT Provider.

This approach would not limit the obligation in APP11 to the specific steps listed in the new regulation, as '*such steps as are reasonable*' in APP11 may require additional actions to be undertaken. However, it would help establish a strong baseline for the obligation while avoiding locking in a low required standard.

The new regulation should be updated regularly with guidance from the ACSC, with the intention of 'ratcheting up' the required cyber security steps over time as the threat landscape evolves. In updating the regulation, regard should be given to maintaining consistency with international frameworks and guidance promulgated by the National Institute of Standards and Technology (NIST) and the international standard ISO27001.

An obligation on IT Providers to comply with APP11 (as modified per the above) should be implied by statute into all contracts between IT Providers and their customers under which the IT Provider stores personal information (as defined in the *Privacy Act*).

©National Australia Bank Limited

An IT Provider's failure to comply with APP11 (so amended) may then result in contractual liability to the IT Provider's customer and to data subjects under the *Privacy Act*. This would cumulatively increase incentives for IT Providers to improve cyber security practises, and particularly to ensure that at least the specific steps enumerated in the new regulation are taken.

If required, this regime could be limited to customers of IT Providers who are consumers or 'small business' (as defined in the Australian Consumer Law). However, even larger enterprises experience difficulties with IT Suppliers in relation to these issues and such a limitation would diminish the effectiveness of this strategy overall.

Review of obligations to retain personal information

Another way to mitigate the potential impact of cyber breaches is through a thorough review of regulatory obligations, which require the retention of records containing personal information, or government identifiers (for instance driver's licences and passports). Customer information is important, particularly in a sector such as banking. There needs to be a balance, however, between maintaining sufficient customer information and avoiding the unnecessary collection of information or storage of records for longer than is necessary.

Further, the creation of an interoperable digital ID ecosystem would also assist, in some cases obviating the need for businesses to collect or keep copies of identification documents which could cause harm to individuals if disclosed. For example, where entities were permitted to rely on zero knowledge proofs (i.e., it is sufficient that an entity knows that an individual is over 18 years old and does not need to collect actual date of birth details or evidence thereof), this would minimise the data security risk to both businesses and individuals. Where a business could maintain a record that an attribute has been verified through a digital ID solution (i.e., that an individual is over 18 years old), that information would not be useful in the hands of cybercriminals, and therefore the harm occasioned by affected individuals would likely be reduced substantially. This would require that existing Digital ID standards and protocols be significantly uplifted. The current regime is not yet fit for purpose. NAB will continue working with federal and state/territory governments to support this.

Recommendations:

- *NAB recommends that Government strongly encourage CTIS participation for all large Australian organisations, given its importance as a source of intelligence.*
- *NAB would welcome further Government work with the telecommunications and other sectors on a mandated Clean Pipes program, designed to ensure the country's internet traffic is cleansed from known-malicious activity.*
- *NAB recommends Government adopt minimum cyber security standards for IT Providers who form part of a business's supply chain.*
- *In line with the Attorney General's recommendation 21.6 in the Privacy Act Review Report, NAB supports a review of the regulatory obligations on business to retain the personal information of customers, particularly in relation to documents which contain government identifiers (for instance driver's licences and passports).*

2. Clear and streamlined regulation

Clear and streamlined regulation will support business to tackle the sophisticated transnational cybercrime industry that continues to thrive.

Various elements of *the Security of Critical Infrastructure (SOCI) Act, Privacy Act*, *CPS 230* and *CPS234* have overlapping requirements, including in relation to data breach or security incident reporting; with each

requirement having differing triggers and timeframes. Notifying and subsequently liaising with multiple regulators during an organisation's response to a cyber event could prove to be confusing, and a distraction from effective operational response to the incident.

Question 2b. Is further reform to SOCI Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

The focus of SOCI is continuity of 'critical infrastructure' as opposed to providing a regime for data protection. The latter is addressed in the *Privacy Act*.

NAB considers that SOCI is broadly fit for its purpose, and should be retained in its current form, subject to the harmonisation recommended in this submission.

Any further redress in relation to the protection of personal information should be addressed in the *Privacy Act*. In March 2023, NAB provided a submission on the Consultation on the Privacy Act Review Report, proposing the introduction of 'a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. The provision would contain safeguards to ensure that only limited information could be made available for designated purposes, and for a time limited duration. Similar to the emergency declaration provisions that exist under Part VIA of the Act, and discussed in Chapter 5, there would be benefit in providing greater flexibility under the Act to permit the sharing of personal information in limited circumstances to respond to a significant data breach'.

2d. Should Australia consider a new Cyber Security Act?

As cited in NAB's submission on the Employment White Paper (November 2022), all levels of Government need to continually assess the regulatory burden they place on business, removing regulation where they can and, where needed, investing in (technology) solutions that make compliance more efficient. Australian business owners increasingly understand the deleterious impact of lax cyber security protocols but are similarly constrained by rising costs and labour shortages. More consistent and streamlined cyber security regulation is required and will be welcomed, but this could be achieved through review and harmonisation of existing regulatory instruments. We are concerned that adding to this framework with an additional comprehensive single Cyber Act risks creating further confusion, without providing clarity on implementation-level guidance of cyber obligations.

2c. Should the obligations of company directors specifically address cyber security risk and consequences?

Effective governance relies on directors who apply rigorous reviews and assessments of business programs and practices. The *Corporations Act (Cth)* was tested in late 2022 to ensure Australian Financial Services licensees are required to have adequate risk management systems in place to manage cyber security risks. This Federal Court ruling, in addition to recent ASIC Guidance[2] and a director's duty to act with care and diligence (*s180)* provides business with clarity in this area and constitutes sufficient regulation[3].
Additional specific cyber security obligations on directors would beg the question as to why the numerous other areas implicitly addressed in *s180* are not enumerated specifically. This could have significant unintended consequences in terms of narrowing the operation of *s180*, to the detriment of Australia in relation to other requirements. Furthermore, under Prudential Standard CPS 234, APRA-regulated entities must take measures to be resilient against information security incidents, including cyber-attacks by maintaining an information security capability commensurate with information security vulnerabilities and threats. Under this Prudential Standard, the Board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security, including appropriate cyber defences.

[2] Cyber resilience good practices - ASIC

[3] 22-104MR Court finds RI Advice failed to adequately manage cybersecurity risks | ASIC

©National Australia Bank Limited

3. Supportive government-industry frameworks

Question 15.a What assistance do small businesses need from government to manage their cyber security risks to keep their/customers' data safe?
Supportive government-industry frameworks are needed to help businesses to respond quickly and confidently in a cyber crisis, such as safe information sharing and exclusion from legal liability in certain circumstances.

This is particularly pertinent to small and medium businesses and varies according to industry type. Recent NAB Economics research showed the number of businesses impacted by a cyber-attack or data breach ranged considerably by industry. Notably, some of the industries that recorded the highest number of attacks (e.g., construction) were also the industries that felt the least prepared and spent less on prevention and training (relative to other sectors). Similarly, the Australian Strategic Policy Institute notes 'the bulk of Australian people and businesses fall into a third category: they would like to defend themselves online but don't have the expertise or the resources to do so'[4].

Our recommendations above in relation to new regulation of IT Providers would be helpful for small businesses to manage their cyber risks. The guidance provided in the new regulation would also provide helpful pointers to small businesses in relation to their own compliance.

Question 7. What can government do to improve information sharing with industry on cyber threats?
Question 8. During a cyber incident, would an explicit obligation of confidentiality upon the ASD/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?

Safe Harbour
The ACSC is critical to our national response to cyber incidents. It is the nation's most important asset in protecting Australian businesses and individuals in a critical situation and building cyber resilience. It has a national footprint of Joint Cyber Security Centres enabling collaboration with partners across the private and public sectors. Free collaboration and frank information sharing with the ACSC is essential to optimising immediate operational response to incidents and leveraging broader government capability. The ACSC should be protected from entanglement with other regulatory or investigative agencies seeking to review the conduct of businesses. Doing so would encourage full, frank and prompt disclosure by businesses who are being attacked.

To that end, NAB recommends that a legislated safe harbour be introduced whereby information can be provided to the ACSC during the course of the operational response. As noted above, NAB supports a change to the *Privacy Act* which would permit the sharing of information in such an event. The ACSC would not be permitted to disclose to other government entities who may use the information for investigations or imposition of consequences following a cyber security incident and would otherwise keep the information confidential.

Without this safe harbour some businesses may be reticent to disclose information which may result in liability, or delay provision of such information until accompanied with additional information aiming to provide defensive or excusing context.

All other required notifications should be harmonised through each relevant department or regulator adopting consistent notification triggers and timelines in the regulations and regulatory instruments that they are responsible for. This would likely require amendment of various pieces of existing legislation,

[4] Clean pipes: Should ISPs provide a more secure internet? | Australian Strategic Policy Institute | ASPI

regulations and regulatory standards. Such amendment is preferable to creation of a consolidated Cyber Act, which may result in further duplication and confusion.

Government should also establish a single interface for notifications required to government entities. Government should then appoint a particular regulator as the leading regulator in relation to each incident, who where practicable will be the enduring point of contact with the business making the notification in relation to further regulation. The leading regulator could be determined by the National Office for Cyber Security or guidance published on who the lead regulator will be for particular industry sectors.

Adopting changes that are consistent with global reporting requirements, in terms of timeframes and criteria, across various regions will help to reduce the compliance burden on business and increase adherence.

Question 2f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by victims and or insurers, and if so under what circumstances?

NAB does not negotiate with criminals and is subject to various legal considerations such as AML legislation that may prohibit ransom payments. However, punitive actions, such as imposing fines, on organisations who have been subject to devastating ransomware attacks is in no way restorative but imposes further impact on the victims. Indeed, we must not punish the victims. Rigid regulation is likely to cause some businesses to elect to pay the ransom without reporting the attack (as non-payment could end the business altogether).

In seeking to protect SME customers with new regulation, Government should carefully consider the compliance impact on these businesses. NAB's business customers are clear that burdensome cyber security compliance requirements will be counterproductive.

NAB works to support and upskill our small business customers to help them comply with any new requirements and elevate their compliance practices. Our ongoing role supporting small and medium businesses to transition to new compliance regimes illustrates our broader commitment to industry-wide improvements.

Recommendations:

- *NAB recommends that a legislated safe harbour be introduced whereby information can be provided to the ACSC during an operational response. The ACSC would not be permitted to disclose this information to other government entities who may use it for investigations following a cyber security incident and must otherwise keep confidential.*
- *Government should also establish a single interface for notifications required to government entities. Government should then appoint a particular regulator as the leading regulator in relation to each incident. This could be determined by the National Office for Cyber Security or guidance published on who the lead regulator will be for particular industry sectors.*

4. Boosting community awareness and education

Question 12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

NAB's 8.5 million customers and 34,000 colleagues are experiencing first-hand the rise of scams and cyber security breaches. Be it a personal banking or business customer, people are looking to large organisations like NAB to provide guidance as they navigate a dynamic digital world. NAB's 'See Through Scams'

campaign uses various platforms to raise awareness on the latest scams and cyber security issues, and the ABA has recently launched a campaign called 'Hear the Alarm Bells' to educate customers[5].

Co-designed awareness projects by Government with industry will help limit the impact of cyber events that affect the health and wellbeing of Australians every day.

The ACSC excels at providing best practice guidance for consumers, including individuals, small businesses, and large organisations. At NAB we have amplified their voice in our communication campaigns. A Government-initiated consumer targeted campaign would benefit all Australians and NAB would be happy to provide support for the campaign.

NAB has a role in educating and improving cyber awareness for small businesses. NAB is partaking in a Small Business Cyber Uplift program with Microsoft and the Council of Small Business Organisations Australia (COSBOA). This program provides cyber security students at TAFE the opportunity to apply theoretical knowledge in a small business setting. Students conduct a high-level cyber security maturity assessment for a small business and provide them with industry-approved advice on how to improve their resilience. This program will be piloted first in Victoria with funding from the state government.

Depending on the pilot outcome, there may be an opportunity to co-brand these initiatives as a nationwide joint activity between Microsoft, NAB, COSBOA and the Federal Government, through the ASD's ACSC.

Recommendation: *NAB supports boosting community awareness and education through a co-designed program led by Government with input from industry. An integrated nationwide program will help to uplift the efforts of individual organisations.*

5. Developing cyber skills

Question 11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Australia's cyber skills shortage is a concern. The National Skills Commission (NSC Annual Report 2020-2021) reported the demand for data and digital skills is widespread and continuing to grow across the economy, and that almost nine in 10 jobs require digital skills – across every sector and every industry[6].

The Australian Government has committed to 1.2 million tech jobs by 2030[7]. NAB supports this ambition outlined by the Minister for Industry and Science, the Hon Ed Husic MP, however, industry needs a much stronger pipeline of prospective students pursuing tech careers to achieve these sorts of targets.

To address this talent shortage, which is part of a broader STEM skill deficit, the earlier introduction of cyber education in schools is imperative. NAB encourages Government to keep increasing its focus on national initiatives such as teaching cyber skills to improve resilience at a grassroots level. A focus on lifting female participation is also necessary, as are industry proposals to develop and pilot programs for mid-career and mature age workers, noting that the absence of digital and cyber skills is increasingly a barrier for participation in meaningful and consistent employment. These programs could include financial support from government and a framework for recognition of work-related training and credentials.

The success of 'lifelong learning' programs overseas (such as Singapore) provide examples of models that could be leveraged locally. NAB would welcome the opportunity to partner with government to address the digital and cyber skills gap for mid-career and mature age workers.

[5] Scams - Hear the alarm bells - Australian Banking Association (ausbanking.org.au)
[6] READY, SET, UPSKILL: EFFECTIVE TRAINING FOR THE JOBS OF TOMORROW - RMIT 2022
[7] Mapping out Australia's path to tech jobs future | Ministers for the Department of Industry, Science and Resources

©National Australia Bank Limited

NAB is a partner of the Grok Academy, along with ASD, who create web-based cyber security challenges for primary and high school students. These initiatives could be formally integrated by Government into the national school curriculum.

Vocational training can provide students with skills for a career in cyber security, mitigating the need to study for three or four years to obtain tertiary degrees. Nation-wide initiatives where government, academia, and industry collaborate to deliver vocational programs would accelerate entry into the cyber jobs market. Course design should be developed to meet the needs of the labour market and emerging cyber skills.

Industry also has a crucial role to play in ensuring Australians have the skills for the future, by way of partnering with universities, vocational and industry education providers. NAB has a strong track record of investing in upskilling and reskilling programs, demonstrated by our formal banking qualification offered through FINSIA to all colleagues and climate training for agribusiness bankers.

Inspiring students to study these fields by showcasing the careers available and types of projects being delivered, such as those in banking and finance, is part of the answer.

Recommendation: *NAB would strongly support and partake in initiatives to develop the required skills and pipeline. Further, we would welcome an opportunity to influence course design, length, content, and structure to meet industry needs.*

Conclusion

Business needs supportive, integrative frameworks that enable it to easily incorporate cyber security risk as an everyday part of decision-making. Sustained cyber resilience is critical to national productivity and ultimately, Australia's security in an evolving digital age. NAB appreciates the opportunity to contribute to this important discussion and we look forward to ongoing engagement on this topic.

Yours sincerely,

Patrick Wright
Group Executive, Technology and Enterprise Operations
National Australia Bank

©National Australia Bank Limited