NATIONAL AUSTRALIA BANK SUBMISSION

2023 – 2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms

March 2024

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

Introduction

National Australia Bank (**NAB**) welcomes the opportunity to respond to the Department of Home Affairs (**Department**) consultation on the 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms (**Consultation Paper**).

NAB's response and focus is guided by the sections in the Consultation Paper. NAB has focused on the key measures of most relevance to NAB.

As a member of the Australian Banking Association (**ABA**), NAB has contributed to their submission to the Consultation.

This submission builds on NAB's engagement in the Government's Cyber Security Strategy consultation process, including our response to the Australian Cyber Security Strategy (2023-2030) Discussion Paper in April 2023.

Executive summary

NAB welcomes the Government pursuing legislative reform to address regulatory gaps and to amend the Security of Critical Infrastructure Act 2018 (Cth) (**SOCI Act**) to strengthen protection of Australia's critical infrastructure. NAB agrees legislative reform is required, and supports the intention to improve the legal and policy frameworks critical to effective cyber security. NAB acknowledges the criticality of the role that the Government has played, and will continue to play, in navigating and addressing cyber threats.

NAB supports several of the proposals made in the Consultation Paper. Ensuring public trust and understanding in Australia's cyber strategy and regime is critical. The success of these legislative reforms depends on ensuring the continued safety and protection of consumers' personal information. For businesses to operate effectively, the Government should strive to ensure uniform and consistent regulatory requirements across the various legislation that governs cyber, data security and privacy. Clear and consistent rules will help foster public trust and confidence in the regime.

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

No feedback provided.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

NAB supports the creation of a mandatory ransomware reporting obligation for ransomware and cyber extortion. The mandatory reporting obligation will support the broader economy and businesses in threat mitigation, through the sharing of up-to-date anonymised data under this obligation. However, consideration should be given to existing mandatory cyber incident reporting obligations, such as Australian Prudential Regulatory Authority's (APRA) Consumer Prudential Standard 234 and the SOCI Act, which requires critical infrastructure owners to report critical incidents (including ransomware and cyber extortion incidents) within 12 hours, followed by a written report within 84 hours of the initial incident. Consideration of existing reporting obligations will assist in reducing regulatory complexity and duplication of reportable information. In turn, this should lift public confidence that breaches are being dealt with swiftly, and with the greatest capability available through Federal Government.

Question 8 – What mandatory information should be reported if an entity has been subject to a ransomware or cyber extortion incident?

NAB suggests information reported should reflect the intent of the regime to improve responsiveness to cyber incidents, mitigate consequences to entities and individuals, and build resilience towards ransomware and cyber extortion threats. Consideration should be given to ensuring these requirements do not impose unnecessary reporting obligations, particularly during an incident. The following information would be beneficial in the mandatory reporting obligation:

- Identity or purported identity of threat actor
- The demand or summary of the threat (e.g. release of data or service interruption)
- The different extortion strategies used by the threat actor (e.g. encryption, data leakage, denial of service, contacting customers, contacting regulators, etc.)
- Timeframe for payment (once known). This could be the initial timeframe and any subsequent extensions for payment through negotiations, and
- Vulnerabilities in the entity's system exploited by the attack (if known).

Question 9 – What additional information should be reported if a payment is made?

If a payment is made, the following additional information would be useful:

- Date of payment
- Amount paid
- Wallet address or any other relevant information of the payment recipient.

Any information, however, pertaining to potential payments should be kept confidential.

Question 10 – Which entities should be subject to the mandatory ransomware reporting obligation?

NAB recommends all businesses and companies (except sole traders) that operate within Australia should be subject to the new mandatory reporting obligation. This is consistent with the notion of the smallest or most vulnerable link often being the entry point for bad actors. However, NAB recognises that in some cases, the increased regulatory burden on small businesses would be challenging and many small businesses may not be in a position to absorb the additional reporting obligation. NAB encourages further consultation with industry on the viability of mandatory reporting obligations for all small businesses.

Question 11 – Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10m per year?

NAB appreciates the Government's consideration of limiting ransomware reporting obligations to larger businesses, which would reduce the impact on small and medium enterprises (**SMEs**). While NAB supports the exclusion of sole traders from the ransomware reporting obligation (regardless of annual turnover), excluding businesses with a turnover of less than $10m could deny Australia vital intelligence on threat actors targeting smaller businesses. Any such exemption could, over time, potentially create an attractive target group for threat actors, which could make it harder to minimise and mitigate these attacks in Australia. In some instances, small businesses can also be the entry point for infiltration of larger business, which is why NAB considers that all businesses, regardless of turnover, should be captured. However, consideration should be given to the scope of reporting obligations necessary for smaller businesses, noting resource and capacity constraints specific to SMEs.

NAB encourages the Department and the Australian Cyber Security Centre (**ACSC**) to provide additional guidance, resources and support to small businesses, including further clarification on reporting requirements, timeframes and available assistance to build their cyber resilience.

As Australia's largest business bank, NAB is also committed to help upskill small business customers to comply with new legal requirements, and elevate their cyber protection practices. NAB can play a key role in assisting SMEs to incorporate cyber compliance into their organisations, while leveraging existing relationships to understand what support our customers require for the transition.

Question 12 – What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?

NAB suggests the time period for reporting should reflect the intent of the regime; which is to provide a clear threat picture of cyber incidents and allow action to be taken to deter criminal groups from targeting Australian entities; but also take into account the level of detail required in reporting by an entity. NAB recommends a minimum of 14 days be allowed for an entity to submit a report after either being subject to a cyber extortion attack or a ransom being paid.

Question 13 – To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident to Government?

NAB believes the introduction of the no-fault and no-liability principles would provide increased confidence and support to entities reporting a ransomware or cyber extortion incident to Government. However, NAB seeks further clarity on whether these protection principles are intended to cover ransomware payments where sanctions are in place (for example, against a ransomware group or region). Further clarity would also be welcome on how the Government intends to proceed with provisions of confidentiality and information sharing in respect of such incidents reported to Government in compliance with this proposed obligation. For instance, NAB considers there is a risk of a class action or law firm seeking to access and use the reporting database to identify and target entities for litigation, via a freedom of information (FOI) or judicial process.

NAB strongly encourages the Government to consider limitations on the disclosure of information that identifies the impacted entity or any individuals when responding to FOI requests or pre-action legal applications. This would not impact the standard legal processes available to class actions and law firms, through which they can request information directly from an entity.

NAB also urges the Government to consider the information provided under the mandatory reporting obligation to be classified under the Protective Security Policy Framework (**PSPF**) Information Security classification. This would ensure only Government employees with a need to know would have access to the data, which may include vulnerabilities to impacted entities.

Question 14 – To what extent would the no-fault and no-liability principle balance public expectations that businesses should take accountability for their cyber security?

The no-fault and no-liability principle is a positive step in balancing an entity's accountability as well as public expectations of accountability. It is reasonable and proportionate to encourage a high level of reporting compliance by relevant entities and should maximise the benefit of the reporting obligations. Other mechanisms are available to hold reporting entities accountable for their actions, including the Privacy Act 1988 (Cth) and, in the financial services industry, the prudential standards relating to information and systems security.

Question 16 – What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, with whom, and in what format?

The following information about ransomware incidents would be helpful for industry to receive:

- Relevant information on the threat actor, including location and any affiliations
- Motivation of the threat actor (where known)
- Amounts paid / claimed, and
- Nature of the threat / category of vulnerability exploited.

A collated monthly update (which entities can subscribe to) would be helpful when dealing with ransomware and cyber extortion incidents. This aligns with NAB's suggestion of a minimum of 14 days as an appropriate period for an entity to submit a report (see response to Question 12).

NAB also recommends publication of an annual report, including key trends (broken down by industry and business size) and any additional information that might help businesses strengthen their own cyber security defences. Breaking down key trends by sector would provide valuable and relevant insights for industries as they prepare for potential cyber-attacks.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

NAB supports a limited use obligation, which will encourage entities to submit timely and accurate reporting in relation to ransomware and cyber-attacks. Up-to-date reporting and information will be crucial in helping uplift Australia's cyber security landscape and will help the Australian Signals Directorate (**ASD**) and the National Cyber Security Coordinator (**Cyber Coordinator**) minimise harm to individuals and businesses.

Question 17 – What should be included in the 'prescribed cyber security purposes' for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?

The following could be included in the 'prescribed cyber security purposes' for a limited use obligation:

- Gathering intelligence and the disruption of activities in relation to threat actors
- For use in the sanctioning and prosecuting or otherwise taking enforcement action against threat actors
- Identification of common vulnerabilities, and
- Communication of anonymised intelligence about common vulnerabilities and mitigating actions to Government and entities.

NAB seeks further clarity on the prescribed purpose of 'consequence management' which has been listed as a permitted use. This could be contrary to the Government's stated intent of encouraging greater information sharing to improve the cyber security landscape.

Question 18 – What restrictions, if any, should apply to the sharing of cyber incident information?

NAB recommends information that might enable identification of an impacted entity not be shared. Sharing should apply to law enforcement and intelligence bodies only and be limited to the purposes outlined in our response to Question 17.

As stated in NAB's response to Question 13, the disclosure of any identifiable information in relation to reporting entities should be excluded from responses to FOI requests and any pre-action legal applications.

Question 19 – What else can governments do to promote and incentivise entities to share information and collaborate with the ASD and the Cyber Coordinator in the aftermath of a cyber incident?

NAB believes timely and practical assistance from ASD and the Cyber Coordinator will help promote and incentivise sharing of information.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

NAB supports the creation of a Cyber Incident Review Board (**CIRB**) to retrospectively investigate and review the root causes of cyber incidents and assess the effectiveness of post-incident responses. Given the high-profile nature of cyber-attacks and changing public expectations, identifying and sharing lessons learned will help contribute to a stronger and more resilient cyber landscape in Australia.

NAB encourages the CIRB to consider industry collaboration through partnerships as one way to enhance cyber capability across the economy. NAB would be prepared to participate should the membership of any CIRB include scope for industry representatives.

Question 20 – What should be the purpose and scope of the proposed CIRB?

NAB believes the CIRB should have a similar remit to the United States Cyber Safety Review Board (**CSRB**), which reviews particular threat actors (e.g. Lapsus$) and particular vulnerabilities (e.g. Log4j) and provides a 'year in review' report.

NAB does not believe the CIRB should have the power to undertake a review of a cyber incident affecting individual entities in Australia (for example, incidents impacting Optus or Medibank).

Question 22 – How should the CIRB ensure that it adopts a 'no fault' approach when reviewing cyber incidents?

As outlined in NAB's response to Question 20, we believe the CIRB's remit should focus on providing an independent view on lessons learned and recommendations on how to improve cyber readiness. This would help ensure a 'no fault' and generalised approach.

Question 30 – To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?

NAB agrees the CIRB should be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator.

Measure 5: Amendments to the Security of Critical Infrastructure Act 2018

Question 35 – How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?

NAB does not consider the proposed amendments are necessary. While not explicitly stated, the SOCI Act already captures data storage systems which could cause significant disruption or damage to critical infrastructure. Given the level of generality of the existing definitions, adding additional reference to data storage systems may create further confusion as there may be other specific examples not identified, leading to uncertainty on whether those examples fall within the more general definitions.

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers

NAB supports the objectives of the proposed consequence management powers as a power of last resort. However, there should be an obligation on Government to minimise the extent and duration of directions to only what is necessary to mitigate material impacts of a cyber incident on entities and Australians.

Question 37 – How would a directions power assist you in taking action to address the consequences of an incident?

The directions power may assist NAB to take action to address consequences of an incident which might otherwise constitute a breach of law (e.g. Privacy Act), prudential standards or contractual obligations (for instance confidentiality obligations to a third-party supplier). These directions power could enable a quicker and more pragmatic response to incidents, thereby reducing harm to customers and the economy.

Question 38 – What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?

Given the complexity of the banking system and associated regulatory frameworks, any direction given to a financial institution should be made in consultation with APRA, ASIC and AUSTRAC. This would help ensure that the contemplated action is taken in a way that minimises (or at least takes into account) impact within the areas of concern of those regulators, such as consumer protection, financial system stability, and AML/CTF requirements. This would also help minimise concerns that regulated entities could face sanctions from other regulators.

Question 39 – What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

There are a range of factors that need to be considered when contemplating the practical application of the consequence management power. For example, directions given to an entity under this power may require the breach of a contract or be contrary to an entity's commercial interests and involve additional costs being incurred.

In the instance of additional costs being incurred as a result of complying with this power (above what may be necessary to protect the interests of NAB and its customers), NAB seeks further clarity on the Government's intention with respect to compensating entities. NAB also encourages the Government to consider specific immunity for entities in relation to any consequent breach of law due to compliance with directions given. This immunity would not extend to any legal consequences from other breaches of the entity's obligations (for instance in relation to cyber security under existing laws, including the SOCI Act itself).

Further consultation on appropriate principles, safeguards and oversight mechanisms will be important as the design and implementation of the consequence management power is finalised.

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions

No feedback provided.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

No feedback provided.

Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act

No feedback provided.

Conclusion

Thank you for the opportunity to provide comments on the Consultation Paper. Strengthening and improving Australia's cyber security laws is vitally important and NAB looks forward to ongoing engagement with the Government on this topic. NAB is more than happy to discuss any aspect of this submission with the Department.