14 April 2023

Expert Advisory Board
Australian Cyber Security Strategy
Department of Home Affairs

Via webform on homeaffairs.gov.au

To the Board

Consultation on 2023-2030 Australian Cyber Security Strategy Discussion Paper

COBA appreciates the opportunity to contribute to the Government's consultation on the *2023-2030 Australian Cyber Security Discussion Paper* (the Discussion Paper).

COBA is the industry association for Australia's customer owned banks (mutual banks, credit unions and building societies). Collectively, our sector has over $160 billion in assets and is the fifth largest holder of household deposits. Customer owned banks account for around two thirds of the total number of domestic Authorised Deposit-taking Institutions (ADIs) and deliver competition and market leading levels of customer satisfaction in the retail banking market.

Key points

COBA supports the development of the 2023-2030 Australian Cyber Security Strategy (the Strategy).

COBA is concerned that extending the definition of "critical assets" to include "customer data and systems" risks bringing smaller banks (i.e., our sector) into the costly obligations under the *Security of Critical Infrastructure Act 2018* (SOCI Act) despite being APRA-regulated and significantly smaller than their peer entities.

The customer owned banking sector is already subject to APRA's prudential standards and supervision, including under CPS 234 Information Security on cyber security.

COBA supports the threshold for qualifying as "critical banking assets" continuing at the current level of $50 billion in assets.

COBA has consistently supported sensible measures to protect Australia's critical infrastructure and systems and is supportive of the Australian Government's development of the updated Strategy. We recognise that the functioning of Australia's banking system is dependent on a secure cyber environment. Our members appreciate the risk posed by the evolving nature of cyber threats and we note that responding to these risks is a high priority for our sector. Our members dedicate considerable resources towards maintaining and developing defences against these threats and to ensure that they are compliant with existing cyber security obligations under various frameworks.

Suite 403, Level 4, 151 Castlereagh Street,
Sydney NSW 2000

Suite 4C, 16 National Circuit,
Barton ACT 2600

Customerownedbanking.asn.au

Customer Owned Banking Association Limited ABN 98 137 780 897

Question 2(b) – definition of critical assets

We, however, would like to address question 2(b) of the Discussion Paper which asks whether to extend the definition of "critical assets" to include "customer data and systems". We are concerned that the change could have unintended consequences by bringing smaller banks (i.e., customer owned banks) into the definition of "critical assets" and therefore into the scope of costly obligations of the SOCI Act.

The threshold to qualify as critical banking assets and subject to the SOCI Act obligations is currently set at $50 billion of total assets. Given there are no customer owned banks over this threshold, it excludes the entirety of our sector and strikes the right balance in capturing those ADIs that are properly considered critical to the Australian banking system. Those banks that exceed the threshold have considerable assets and provide banking services for a significant proportion of the Australian population.

While the customer owned banking sector has over $160 billion in assets, these are spread over 58 ADI institutions with our sector still considerably smaller than each of the major banks. COBA members range in size from approximately $15 million in total assets for our smallest member to around $25 billion in total assets for our largest member.

While our member banks are currently not subject to the SOCI Act obligations, they are still subject to extensive regulation and supervision on cyber security as APRA-regulated entities. APRA's prudential regulatory requirements include legally enforceable prudential standards that specifically address risk management, business continuity management, and information security, which includes responding to cyber attacks. APRA's recent supervisory priorities highlight its increased focus on cyber security (CPS 234) outlining that "improving cyber resilience remains a key cross-industry supervision priority for APRA", that it will exercise "heightened supervision", and that a key part of its cyber strategy is to "uplift cyber resilience across the financial sector."[1]

Question 2(g) – clarity on the payment or non-payment of ransoms

COBA supports greater clarity on the Government's position with respect to payment or non-payment of ransoms by companies as well as the circumstances in which this may constitute a breach of Australian law.

We look forward to engaging with the Department on this issue and thank you for taking our views into account. Please do not hesitate to contact Robert Thomas, Senior Policy Adviser (rthomas@coba.asn.au) if you have any questions about our submission.

Yours sincerely

MICHAEL LAWRENCE
Chief Executive Officer

[1] See APRA's 2023 Supervision Priorities.