

1 March 2024

Expert Advisory Board
Australian Cyber Security Strategy
Department of Home Affairs

Via portal: homeaffairs.gov.au

To the Board

Cyber Security Legislative Reforms Consultation

COBA welcomes the opportunity to comment on the Department of Home Affairs *2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper*.

COBA represents Australia's customer owned banks (mutual banks, credit unions and building societies). Collectively, our sector has over \$170 billion in assets, around 10 per cent of the household deposit market and around five million customers. Customer owned banking institutions account for around two-thirds of the total number of domestic Authorised Deposit-taking Institutions (ADIs).

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.

Key points

COBA supports the Government's Cyber Security Strategy 2023-2030 and in general the proposals made in this Consultation Paper.

COBA supports ransomware reporting for businesses, and we believe that for banks these measures are most appropriately addressed under APRA's CPS 234 Information Security. In line with this, the Government should ensure that it does not create any unnecessary duplication or burden in its ransomware reporting regime for smaller banks.

COBA has consistently supported sensible measures to protect Australia's critical infrastructure and systems. We are supportive of both the 2023-2030 Australian Cyber Security Strategy and the measures that are proposed in this Consultation Paper. Our sector recognises that the functioning of Australia's banking system is dependent on a secure cyber environment. As such, our members dedicate significant resources towards maintaining and developing defences against these threats and to ensure compliance with existing cyber security obligations.

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

Suite 4C, 16 National Circuit,
Barton ACT 2600

[Customerownedbanking.asn.au](https://customerownedbanking.asn.au)

Ransomware reporting for businesses

COBA thanks the Government for clarifying its view on the payment or non-payment of ransoms by companies and for clearly indicating its position on the prosecution of businesses that pay the ransom. We agree with the Government's position where it discourages businesses and individuals from paying ransoms to cyber criminals as we believe that this is the only appropriate response to these kinds of attacks. However, we also appreciate that the Government clearly articulating its position on prosecutions will encourage full and cooperative reporting by businesses whenever these attacks occur regardless of whether a payment is made.

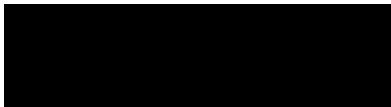
We believe that the proposed measures to provide clear ransomware reporting on businesses appear appropriate as they largely align with pre-existing obligations that apply to banks under APRA's CPS 234: Information Security. Due to the significant overlap between CPS 234 and the proposed measures we ask Government to not duplicate any reporting processes for banks, particularly smaller banks. We ask that APRA be the sole agency to which banks report ransomware incidents rather than needing to provide a duplicative report to Department of Home Affairs. Information that is collected by APRA through these ransomware reports under CPS 234 by banks could then be shared with other agencies as appropriate.

We believe that any ransomware attacks on our members would likely be reported to APRA in accordance with the current provisions under CPS 234. However, if the Government believes that the existing provisions in CPS 234 are not sufficiently clear and do not capture the full intent provided for in the Consultation Paper, then we ask that APRA amend CPS 234 accordingly to ensure its alignment with the broader approach that will apply to other industries.

Additionally, COBA seeks clarification from the Government on how it intends to have the ransomware playbook promised in the Cyber Security Action Plan¹ interact with its proposed ransomware reporting obligations.

We look forward to engaging with the Department of Home Affairs on this issue and thank you for taking our views into account. Please do not hesitate to contact Leanne Vale, Chief of Financial Crimes and Cyber Resilience ([REDACTED]) or Robert Thomas, Policy Manager ([REDACTED]) if you have any questions about our submission.

Yours sincerely



MICHAEL LAWRENCE
Chief Executive Officer

¹ See *2023-2030 Australian Cyber Security Strategy: Action Plan* (2023), 7.