Australian Banking Association

Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Department of Home Affairs

29 August 2025

Table of Contents

Australian Banking Association

Overview

The Australian Banking Association (**ABA**) welcomes the opportunity to make a short submission to the Policy Discussion Paper *Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy* (**the discussion paper**).

The ABA submission focuses on the alignment between existing banking sector regulation (ie. CPS234) and the strategy outlined in the discussion paper. We highlight some areas to streamline the regulatory environment.

Responses to selected questions

1. What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?

The cyber security landscape will continue to evolve, with challenges and opportunities emerging from – among other matters – changing geopolitics, evolving economic and trade patterns, and advancing technology. Noting the unpredictable nature of the evolving threat environment, in our view, one of the key factors for Government consideration is how best to ensure that the Australian retains access to cyber-relevant roles and skillsets.

17. Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?

While the ABA does not suggest that regulatory/compliance requirements have negatively impacted the cyber maturity of our member organisations, there is opportunity for better alignment and harmonisation between Government and industry. Australian banks currently invest significant resources and efforts towards cyber reporting to the Australian Government.

While not downplaying the importance of this reporting, greater alignment and harmonisation would support prioritisation of resources towards frontline cyber-security while also ensuring more effective public-private communication.

Duplication of Incident Reporting Obligations

Australian banks have incident and data breach reporting obligations to numerous Australian Government and related entities. A non-exhaustive list would include:

1. Office of the Australian Information Commissioner (**OAIC**)
2. Australian Prudential Regulation Authority
3. Australian Securities and Investments Commission (**ASIC**)
4. Australian Signals Directorate's Australian Cyber Security Centre (with connected reporting requirements to the Department of Home Affairs)
5. Australian Securities Exchange
6. Reserve Bank of Australia
7. State-based regulators, including privacy and information commissioners

Different regulators will overlap in scope and require different obligations, thresholds, recipients, formats, and data. The outcome of the current landscape is that banks must respond to the same (or only slightly different) questions and requests from multiple regulators for a single incident. The extent to which information is shared within government and by regulators is uncertain. Ultimately, this impacts the capacity of backend systems and staffing to remediate incidents and coordinate responses to the resulting investigations.

\While the Department has commenced developing a single reporting portal for cybersecurity incidents, we view a consistent set of reporting obligations and thresholds would bring benefits across all parties – improving information flows between the private and public sectors and allowing more resources to be dedicated to frontline cybersecurity management.

This duplication is amplified when considering reporting obligations may exist across multiple jurisdictions for entities with operations extending outside of Australia. Large, multinational financial services organisations will likely have multi-jurisdictional obligations in the case of a cyber security breach. These obligations have different reporting timelines, different information requirements and forms they must take. Given large multinational regulated entities must simultaneously grapple with the complexity of the Australian legal framework and international requirements, the need to rationalise the Australian approach is amplified if it is to become the basis for regional cyber security.

Inconsistent Definitions

A corollary of the above is that greater consistency and clarity of data classifications will assist entities in meeting their reporting obligations. Key terms and thresholds vary across different regulatory instruments and legislation and may be subject to conflicting legal and regulatory considerations for the collection, use, storage and retention of data.

Overlapping and duplicative guidance for emerging technologies

Noting that the rapidly moving technological frontier is a key factor shaping the evolving cyber outlook, the ABA suggests that the Australian Government could consider how best to streamline existing guidance and policy responsibilities to ensure that there is a consolidated view across Government. This uncertainty is exacerbated with the multiple reform efforts in these areas (for example, further tranche 2 reforms to the *Privacy Act*, the Department's review of Commonwealth data retention requirements, and the recent review of cyber security legislation). As such, we encourage harmonisation of reforms processes and rationalisation of the outputs of current legislative obligations with the various reform proposals.

By way of illustration, artificial intelligence is the subject of multiple reviews, guidance and inquiries from different Government agencies –OAIC,[1] the Department of Science and Industry,[2] the ASIC,[3] the Cyber and Infrastructure Security Centre,[4] among others.

While Government departments and agencies are bound by their respective remits, obligations and powers, a coordinated and aligned approach across Government would significantly enhance the overall effectiveness of Australia's cyber security.

30. Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?

A non-exhaustive list includes:

[1] https://www.oaic.gov.au/news/media-centre/new-ai-guidance-makes-privacy-compliance-easier-for-business
[2] https://www.industry.gov.au/science-technology-and-innovation/technology/artificial-intelligence
[3] https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-238mr-asic-warns-governance-gap-could-emerge-in-first-report-on-ai-adoption-by-licensees/
[4] https://www.cisc.gov.au/resources-subsite/Documents/artificial-intelligence-factsheet.pdf

- Clear guidance on how Government will engage with industry in the event of a crisis scenario, including sequencing of Government engagement, the identity of the key engagement points, and identification of expected benefits and outcomes.
- Continued cross-industry exercises to build and refine understanding of how this guidance will operate in practice.

36. What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?

Support focused on practical enablement, regulatory clarity and strategic collaboration. This could include further regulatory guidance on the issues outlined above, guidance on integrating *Security of Critical Infrastructure Act* obligations with existing prudential obligations, more standardisation in definitions, further public-private collaboration, among other matters.

Policy Lead: [redacted]

About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.