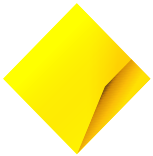
Commonwealth Bank

Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Public Submission

August 2025

Table of contents



1. Executive Summary

CBA welcomes the opportunity to contribute its views to the Australian Government's Discussion Paper *Charting New Horizon – Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy* (Horizon 2).

We continue to support the Government's ambition set out in the 2023-2030 Cyber Strategy (Cyber Strategy) of becoming a world leader in cyber security by 2030. It essential to provide confidence to Australian businesses and consumers, through fit-for-purpose cyber regulations, capacity building and threat-sharing initiatives, so that Australians can engage online with confidence.

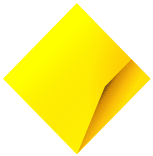
CBA believes strengthening Australia's cyber resilience is key to promoting trust in the digital economy and promoting Australia's economic security, given the significant costs to Australian businesses and consumers from cyber-attacks. Investments in cyber resilience and supporting Government policies are economic productivity measures, not just security costs.

The Cyber Strategy's enduring six cyber shields provide a framework for government and industry to work together in advancement of our collective cyber resilience. The partnership between industry and government will be critical in addressing the evolving threats of the current cyber threat landscape, characterised by heightened geopolitical instability, rapid technological advancement, and growing digital interdependence. These characteristics carry the potential to increase both the velocity of cyber-attacks and magnitude of harms caused to Australian businesses and consumers.

The development of Horizon 2 provides an opportunity to ensure that Australia's policy settings and cyber security posture is fit for purpose, now and into the future.

Priority themes represented in this submission include:

- The need to more clearly define and identify sovereign capabilities, including cyber, to guide industry development, research and commercialisation, and capital allocation as part of a broader integrated national approach to economic resilience that embeds the role of business.
- Ensuring that regulatory frameworks are designed for growth and innovation as well as safety and protection – noting the current mix of regulation between *Security of Critical Infrastructure Act 2018* (SOCI), the *Cyber Security Act 2024*, and sectoral-based regulations such as CPS234 in financial services, currently strikes the right balance.
- The need for Government initiatives directed towards small and medium businesses (SMBs) to evolve from awareness raising to practical action SMBs can take to enhance cyber resilience noting the widening gap between small and larger organisations on cyber maturity.
- Providing greater alignment on public messaging, from government and industry channels, across scams, fraud and cyber threats.
- Prioritising development of the cyber workforce through initiatives directed towards early education, vocational pathways, reskilling programmes and close collaboration between government, education providers, and industry to address the persistent workforce shortfall.
- The expansion in scope and depth of cyber exercises, moving beyond towards cross-sector simulations that include government interaction.
- Support for ongoing whole-of-Government initiatives that will enhance Australian cyber security landscape including Digital ID, Facial Verification Service, prohibition on screen scraping.



CBA looks forward to further engagement with the Government on development of Horizon 2 of the Cyber Strategy and any of the issues raised in this submission.[1]

2. Developing Horizon 2

2.1 Outlook for Horizon 2

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 is being reshaped by geopolitical instability, rapid technological advancement, and growing digital interdependence. These issues and consequences for Australia's national cyber resilience are well documented by the Australian Signals Directorate's (ASD) Annual Cyber Threat Report.[2]

Emerging technologies such as generative AI and quantum computing present both opportunities and risks in the cyber context. AI for example is both enhancing cyber defences in terms of accuracy and efficiency and enabling more sophisticated cyber threats, including automated phishing and malware, while also introducing new vulnerabilities in the form of model manipulation and data leakage. AI-generated fraud and scam threats continue to compromise the safety of Australians in the online environment.

Australia's digital infrastructure, such as 5G networks and digital identity systems, must be treated as strategic assets requiring robust protection. Investment in domestic cloud, compute and satellite infrastructure will be essential to reduce exposure to foreign interference and ensure national resilience.

Beyond geopolitical and technology trends, the Government should also consider the implications of demographic change, including an ageing workforce and the need for continuous reskilling in cyber-relevant roles. These considerations are central to the challenge of sustaining a cyber workforce.

Horizon 2 also provides an opportunity to consider the widening cyber gap between large and small businesses regarding their cyber security. This is a global challenge. The World Economic Forum's latest Global Cybersecurity Outlook 2025 shows that 35% %of small organisations believe their cyber resilience is inadequate, an sevenfold increase since 2022. By contrast, the share of large organisations reporting insufficient cyber resilience has nearly halved.[3] The Australian Government's latest Cyber Threat Report[4] highlights that the average costs of cybercrime for small businesses have increased by 8 %, while the average costs for medium and large business declined.[5]

Cyber capability as a pillar of economic resilience

Strengthening Australia's economic resilience and ability to compete and thrive in an increasingly turbulent, tech-driven world demands a more integrated, whole-of-nation approach – one that positions cyber capabilities not just as a security imperative, but as a strategic economic asset. Large Australian businesses already make outsized investments in nationally significant systems and infrastructure, including cyber. Yet our scale, expertise and assets remain underutilised. A national approach to economic resilience that embeds and amplifies the role of business, investment and markets would unlock new

[1] CBA has not provided responses to questions 20, 46, 47, 48 listed in the discussion paper.
[2] https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024
[3] https://www.weforum.org/stories/2025/01/growing-complexity-global-cybersecurity-from-challenges-action
[4] https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024
[5] This issue is discussed in more detail in responses to questions 7-10.

opportunities to build and sustain digital sovereign capabilities for long-term global competitiveness and help ensure the benefits of the digital economy and AI are not siphoned offshore.

2.2 Collaborating across all levels of government

2. *Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?*

CBA believes a national approach that integrates cyber literacy into everyday learning—supported by practical guidelines and consistent standards—would help build a generation of digitally aware citizens.

At a higher level, there is a strong case for strengthening cyber education into the national curriculum from an early age. The Australian Institute of Criminology's (AIC) Cybercrime in Australia 2023 report, based on a survey of computer users in early 2023, found younger people were more likely to be cybercrime victims than older people. Almost 31 % of respondents aged 18-24 years said they had been a victim of a malware attack in the 12 months prior to the survey. The next highest age group to fall victim were those aged between 25-34 years (24.4 %). The age groups least likely to fall victim were those aged 65 years and older (20.3 %) and 50-64 years (18.5 %).[6] To support the effectiveness of current cyber education in schools, there is a need for teacher professional learning to develop knowledge of cyber awareness and hygiene.[7]

Initiatives that promote cyber education that could be expanded or replicated to lift cyber awareness of school children include:

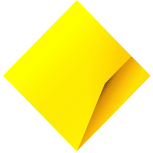
- *Cybermarvel*, an online safety awareness program led the NSW Government has made progress in helping school children understand their digital rights and responsibilities and provides practical guidance to help children and their caregivers use secure apps and devices, review privacy settings, reflect about how actions online may affect others, and how to report online abuse.[8] CBA believes there would be value in replicated this program across other jurisdictions.
- Newer initiatives, such as the Australian Federal Police's *re_BOOTCAMP*, aims to encourage students, with the skills to hack ethically, to pursue positive careers in cyber security by exposing them to opportunities that exist when they use their skills within the boundaries of the law, are welcome.[9]
- International examples such as Estonia's free technical cyber security training and youth-focused Cyber Olympics demonstrate the value of early and accessible cyber education.

A National Cyber Skills Framework would also help align qualifications with specific job roles, ensuring that graduates are equipped with the right capabilities. Currently, a Bachelor of Cyber Security can lead to a wide range of roles without clear expectations or pathways. A more structured approach would support both workforce development and employer confidence.

2.3 Monitoring Progress in a changing world

3. *Does the high-level Model resonate, and do you have any suggestions for its refinement?*
4. *Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?*

[6] https://www.aic.gov.au/publications/sr/sr43
[7] https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=4076&context=ecuworks2022-2026
[8] https://www.nsw.gov.au/education-and-training/cybermarvel
[9] https://www.afp.gov.au/news-centre/media-release/reb00tcmp-inspires-next-generation-cyber-champions



CBA understands the model is intended to be agnostic in relation to the Cyber Security Strategy and not designed to be tied to a single set of actions or cyber shields. However, due to the timebound nature of the Government's Cyber Security Strategy, challenges arise from the Government's planned roadmap for achieving Horizon 2 objectives. CBA would suggest more explicit outcomes metrics that are aligned to strategic objectives of the Cyber Strategy, for example reduction in volume of attacks across consumer and small business that encompasses Shield 1. CBA would welcome additional guidance in due course regarding industry and community involvement in the evaluation process for the strategy.

A more intuitive and structured representation, tied to the framework of the Cyber Security Strategy – namely the six cyber shields, would enhance stakeholders' understanding of the Government's priorities, actions within that thematic, and how they interconnect. This would help to articulate shared government and industry long-term goals and short-term progress. CBA encourages ongoing dialogue regarding the model's development to ensure it supports effective implementation of the strategy.

CBA further notes challenges arising from the absence of defined success measures aligned with the strategy and its objectives. International precedents, such as the U.S. Cybersecurity and Infrastructure Security Agency's "measures of effectiveness" framework, offer valuable examples. Such metrics are instrumental in translating broad goals into specific outcomes and facilitate ongoing assessment of program impact. To promote accountability and monitor progress effectively, strategic objectives should be measurable and informed by stakeholder consultation, incorporating community feedback to ensure appropriate and relevant success measures.

3. Shield-level focus for Horizon 2

3.1 Strong business and citizens

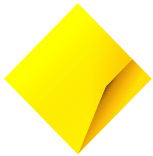
5. *What could government to do better target and consolidate its cyber awareness message?*
6. *What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?*

To improve national cyber awareness, government messaging must be clearer, more consistent, and easier to act on. Australians value clear direction on what they can do to remain safe online - such as recognising phishing attempts, using strong passphrases, and keeping devices updated – and what responsibilities lie with manufacturers of smart devices, service providers, and government. For small businesses, there should be a defined standard that outlines what is expected of them. Established frameworks such as the Essential Eight are often too complex or resource-intensive for SMB and not-for-profits (NFPs), developing a customised standard specifically for them could further address their unique needs and close existing gaps

A unified message across federal, state and territory governments would reduce fragmentation and ensure consistent communication. CBA believes that simplicity is key – cyber security messaging should be short, clear and accessible to all Australians, including those without technical backgrounds. Practical advice could help demystify cyber security and encourage behavioural change.

Government could also draw on behavioural science to improve message effectiveness. For example, loss aversion in terms of highlighting what people stand to lose, has proven to be a strong motivator for action as has gamification in cyber education.[10]

[10] https://research.csiro.au/cybersecurity-quantum-systems/cyber-gamification/



CBA encourages Government to consolidate its cyber education campaigns with fraud and scam awareness, as cyber risks often lead to financial harm through phishing, malware and identity theft. Partnerships with schools and universities can help embed safe technology use as a life skill from an early age. Improving education and awareness amongst older Australians, culturally and linguistically diverse communities, as well as First Nations communities should be a focus as well. This will require communications to be accessible and tailored to the specific needs of these communities.

7. *How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?*

Small businesses and not-for-profits face similar cyber security obstacles. They often have limited financial and technical resources, time constraints, and a lack of in-house cyber expertise. Many are not fully aware of threats or perceive cyber security as too complex, costly, or not an urgent priority.

To enhance our national cyber resilience, the Government could embed proven and effective resources into existing government processes. For example, when renewing an ABN, businesses could receive a tailored cyber information pack outlining current threats and available support. This method would help establish a baseline of security expectations and ensure consistent communication.

CBA believes a core feature of Horizon 2 of the Cyber Strategy should be to facilitate a shift from SMB awareness of cyber issues to action. As part of this priority, the Government could also boost uptake of existing resources by raising awareness, simplifying access, and leveraging trusted channels to promote existing cyber resources. By collaborating with banks, telecommunication service providers, and familiar service platforms, governments can deliver cyber messaging directly within the environments that SMBs already trust. This integration supports a smoother transition to adopting existing cyber resources. Targeted outreach, supported by non-technical language, and further education can ensure SMBs know about Government-funded support programs, such as the Small Business Cyber Resilience Service and Cyber Wardens.

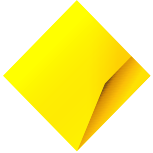
CBA is founding member of an industry alliance that supports the development of Cyber Wardens which makes cyber security simple for small businesses through jargon-free, self-paced, training models.[11] In May 2025, the Cyber Wardens program announced an exclusive collaboration with CyberCert, a globally recognised cyber security certification, offering SMB across Australia a path to enhanced protection.[12]

There are international examples from which the Australian Government can draw to refine support for SMB and NFPs, and drive action to boost cyber resilience.

- The UK's Cyber Essentials certification scheme (backed by government) has seen strong adoption, helping tens of thousands of SMBs implement basic protections and signal security commitment to customers.
- In the US, the Small Business Administration's Cybersecurity Pilot is funding free training and support through state partners, directly assisting SMBs with cyber defences.
- The EU's cybersecurity agency ENISA has published simplified "12-step" security guides and even a joint EU-US cybersecurity checklist to encourage best practices in small organisations.

8. *How can industry at all levels and government work together to drive the uptake of cyber security actions by SMBs and the NFP sector to enhance our national cyber resilience?*
9. *What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's?*

[11] https://www.commbank.com.au/articles/newsroom/2023/08/cybersecurity-wardens-small-business-initiative.html
[12] https://cyberwardens.com.au/media-hub/cyber-wardens-launches-cyber-cert-partnership/



10. *What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?*

At the industry level, trusted channels such as banks and telecommunication providers can also be leveraged to deliver cyber messaging in familiar environments.

CBA has previously worked with the ASD, both on written communication targeted at small businesses via the Signals web content on our website. In addition, CBA has a network of customer-facing staff who interface with small business clients that can opt in to additional cyber training that equips them to deliver cyber education and awareness content to SMB customers focused on understanding risks and threats and the controls that can be applied to help protect information confidentiality, integrity and availability. This program provides a referral pathway to ASD resources.

As noted earlier, CBA believes that current frameworks like the Essential Eight are often too complex or resource-intensive for SMBs and NFPs. Rather than developing Australia-specific standards, it is recommended that the government leverage and tailor existing global frameworks (such as NIST SP 1300). By adopting a common, internationally recognised taxonomy, SMBs and NFPs gain significant advantages: they can more easily align their security practices with those of global service providers and better meet the requirements of international customers. This approach also makes it easier for SMBs and NFPs to tap into global resources, guidance, and support networks, further strengthening Australia's overall cyber resilience.

11. *Do you consider cyber insurance products to be affordable and accessible, particularly for small entities? If not, what factors are holding back uptake of cyber insurance?*

While premiums have softened in recent years, many small and medium businesses still find cyber insurance difficult to access. Affordability remains a challenge, and some SMBs make commercial decisions to forgo insurance due to cost or perceived low risk.

Insurers often require baseline controls such as multi-factor authentication, endpoint detection and response, and tested backups, requirements that many SMBs struggle to meet. The underwriting process can be complex, with technical questionnaires creating additional friction.

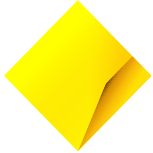
To improve accessibility, government could consider endorsing a simplified cyber standard for SMBs that insurers recognise, making eligibility clearer. At the industry level, linking participation in Government-funded programs like Cyber Wardens to premium incentives could also assist in making cyber insurance more accessible.

12. *How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?*
13. *How could the government further support businesses and individuals to protect themselves from ransomware attacks?*

Ransomware continues to be a significant and evolving threat, particularly for individuals and smaller organisations. ASD reports that of the number of extortion-related cyber security incidents responded to by ASD in 2023-24 increased by 9 % compared to the prior financial year with around 71 % of these incidents involved ransomware.[13]

While awareness is growing, there remains a gap in understanding the full scope of the threat and how it is changing. The Government's reporting on ransomware attacks – currently limited to incidents where

[13] https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024



ransoms are paid – does not provide a complete picture. In time, and as the Government's ransomware reporting framework develops beyond its 'education first approach' in phase 1 through to the end of 2025, CBA welcomes this information, in aggregate, being used to observe what threat actors are most active, what types of entities and businesses they target, what types of code and malicious software (e.g. ransomware, malware, etc.) are used to extort entities and to assist the Government in disseminating tailored advice to industry, particularly SMBs.[14]

CBA believes there is an opportunity to expand government reporting and public education to better reflect the nature and impact of ransomware, including its increasing sophistication and the challenges of recovery. Examples of how ransomware trends are reporting in other jurisdictions include:

- Federal agencies in the United States publicly share ransomware trend data with businesses. The FBI's Internet Crime Complaint Centre (IC3) publishes an annual Internet Crime Report with statistics on ransomware incidents and losses. CISA routinely issues cyber security advisories (often jointly with the FBI and international partners) to alert industry on emerging ransomware tactics and recommended defences.
- The US Government maintains StopRansomware.gov, a one-stop hub consolidating the latest ransomware alerts, trend reports, and best-practice guidance for businesses.
- The UK's National Cyber Security Centre (NCSC) keeps industry informed through both annual reporting and real-time guidance. The NCSC maintains a dedicated "Ransomware Hub" with up-to-date advice and practical resources to help organisations prevent, report, respond to, and recover from attacks. This three-pronged approach – alerting audiences to threats, engaging industries with guidance, and updating best-practice resources – ensures UK businesses receive current ransomware trend information.

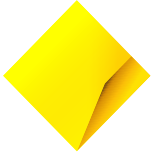
Beyond greater information sharing on the ransomware threat landscape, the Australian Government support could focus on subsidising preventative tools and services, as well as providing assistance during incident response. Many smaller organisations lack the resources to implement robust cyber defences or respond effectively to ransomware incidents. Providing access to secure-by-default software, free penetration testing, and support for resolving vulnerabilities in commonly used platforms (e.g. Office 365, VPNs) would help uplift capability. Additionally, guidance on recovery – not just prevention – should be prioritised, recognising that even well-defended organisations may be impacted.

14. *Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?*

There are examples of certain scams and cyber threats disproportionately affecting specific communities. For example, extortion scams have targeted Mandarin-speaking Australians, the "Hope App" scam disproportionately affected members of CALD communities including recent migrants from Burma and Sri Lanka[15], while university students and regional communities have been affected by targeted scams.

Language barriers and lack of tailored messaging contribute to these vulnerabilities. In response, CBA has developed targeted communications in Mandarin and held in-person seminars in-branch to reach vulnerable cohorts who prefer face-to-face interaction. Broader opportunities exist for government and industry to support inclusive and culturally appropriate cyber education.

[14] https://www.homeaffairs.gov.au/cyber-security-subsite/files/factsheet-ransomware-payment-reporting.pdf
[15] https://www.accc.gov.au/media-release/australians-lose-over-70-million-to-bogus-investment-opportunities



15. How can support services for victims of identity crime be designed to be more effective in the context of increasing demand?

Recovery from identity crime is often extremely difficult for victims, and at times confusing. Victims face different processes and fees depending on their location, and there is no national approach to remediation. Some states, such as NSW and WA, have compromised ID registers, while others do not.

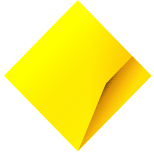
The Australian Government has progressed several significant reforms which will assist consumers to engage safely in the online environment. Given the rise of agentic ecommerce and nefarious AI use-cases deployed by threat actors, such as deep fakes, which can increase the velocity of harms, CBA believes the following reforms should continue to be prioritised and expedited to promote a more secure economy-wide cyber security posture to prevent identity crime:

- Digital ID: In an increasingly digital world, Digital ID systems give consumers trust to engage in the online environment and limits the need for businesses o store identity data, thereby limiting the proliferation of sensitive information and data breach exposure. With the passage of the Digital ID Bill (2024), consumers will have more secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses. The phased expansion of the Australian Government Digital ID System (AGDIS) will enable the reciprocal use of Digital ID and attribute providers in Commonwealth and state and territory services with private entities by December 2026. CBA supports the expansion of Digital ID adoption and the AGDIS scheme itself, noting that it is critical that accreditation standards and AGDIS rules, are fit for purpose for private sector providers.
- Facial Verification Service: The Government passed the Identity Verification Services Act in 2023, establishing a legislative basis for the government's Face Verification Service (FVS) and related identity-matching services. CBA supports the expansion of the regulated use of the FVS beyond government, allowing banks and other organisations to verify identities by matching a person's photo against official IDs with explicit consent. These reforms will enable faster, more secure online ID checks by reducing ID takeover instances for businesses and reinforce privacy safeguards. State and Territory Governments agreed to provide driver licence images under an intergovernmental agreement signed by the Council of Australian Governments in 2017, however currently only Tasmania, Victoria, and South Australia are sharing their data.[16]
- Screen Scraping: CBA welcomes the Government's intention to move towards a ban on screen scraping[17], noting that data aggregators can create detailed profiles of individuals, increasing the risk of identity theft.[18]

16. Which regulations do you consider most important in reducing overall cyber risk in Australia?
17. Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?

As an entity regulated by the Australian Prudential Regulation Authority (APRA), compliance with CPS 230 and CPS 234 is required for managing cyber and operational risk in Australia's financial sector. CPS 234 outlines requirements for information security, including defined responsibilities, incident management, testing, and oversight of third parties. CPS 230 covers broader aspects of operational resilience. The Cyber

[16] https://www.idmatch.gov.au/
[17] https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/consumer-data-right-expansion-deliver-better-deal
[18] This issue is discussed in more detail in response to 21, 22



Security Act 2024 and SOCI Act together provide a broader national framework aimed at enhancing national resilience, incident reporting.

There is an ongoing need to streamline overlapping obligations and improve clarity, particularly for smaller organisations. CBA welcomes the Government's recent work under Horizon 1 of the Cyber Security Strategy to introduce a Single Reporting Portal and looks forward to ongoing engagement on Phase 2 of the Portal's development to identify inefficiencies and options for harmonisation. Aside from the single reporting portal to Government, CBA believes a legislative framework that enables easier information sharing between public and private sectors would also help improve threat response and coordination.

In general, CBA believes regulatory requirements have had a positive impact on cyber maturity. Frameworks like CPS 234 have helped organisations better understand their current posture and prioritise controls. The requirement to align controls with the criticality of information assets has driven more strategic investment in cyber security. While compliance obligations can be resource-intensive, they have also encouraged more systematic testing and assurance. Regulations should remain proportionate and not duplicate existing requirements across different agencies.

3.2 Safe Technology

18. *What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?*
19. *How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?*

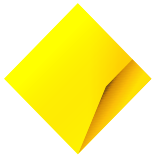
Australia can draw on the work of the UK's National Cyber Security Centre and the US Cybersecurity and Infrastructure Security Agency, both of which provide practical guidance and frameworks for secure technology.

For consumer energy resources and operational technology, regulation should begin at the manufacturing level. Devices should be secure by design, with mandatory patching and software updates as vulnerabilities emerge. Products should not be released to market without basic security features, and where possible, internet connectivity should be limited or discouraged to reduce exposure.

Government has a key role to play in simplifying this landscape through digital safety standards and mandatory compliance for products sold in Australia. For example, just as Domain Name System redirection is used to block illegal content, similar mechanisms could be applied to phishing and malware sites. Internet service providers should be empowered and protected under legislation to implement these protections. Clear labelling, public awareness campaigns, and consistent messaging would also help consumers make informed choices and adopt safer behaviours.

20. *How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?*
21. *Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How does Government and Industry work together to achieve this aim in an evolving global threat environment?*

CBA believes there continues to be a need for more flexible, secure, and timely mechanisms for data sharing to minimise the threat malicious activity and notes data sharing issues are spread across multiple portfolios.



Current privacy legislation can inhibit the ability of organisations to share information quickly, even when it could help prevent or mitigate harm. Government could consider reforms that enable secure, purpose-specific data sharing between trusted parties, particularly in the context of cybercrime, scams, and supporting vulnerable customers. This would support faster detection and response, while maintaining appropriate safeguards for privacy and data protection. To this end, CBA believes reform of the Privacy Act should incorporate a strategic whole-of-government approach to data regulation.

CBA welcomes recent reviews by Government that seek to understand and address the overlapping data retention requirements. In relation to data retention, the regulatory landscape has become increasingly characterised by an ever-expanding range of complex and often conflicting obligations. This is felt particularly acutely in highly regulated sectors like banking. Across the sector, managing these often conflicting, and at times contradictory, obligations is administratively challenging and fraught with regulatory and legal risk. If the outcome of the Commonwealth Data Retention Review, progressed in March 2025 through peak bodies, is to remove repetitive or out-dated retention obligations where possible, this will help reduce privacy and cyber security risks for both individuals and organisations. CBA's views in relation to this review are represented by a submission made by the ABA.

To foster innovation while protecting against exploitation, government and industry must collaborate on secure data-sharing frameworks that are transparent, risk-based and aligned with international standards.

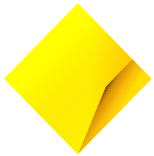
CBA has long been concerned with screen scraping practices which introduce a multitude of risks to consumers and businesses in relation to their data. CBA notes there are various accreditation models under the Consumer Data Right that organisations transitioning away from screen scraping business models can adopt, which facilitate innovation and competition. As the CDR ecosystem has matured, software and platform service providers have grown and enabled modularised CDR solutions, without requiring a ground-up build. This enables benefits such as higher security standards, greater speed to market through streamlined pre-requisites for participation, and promotion of CDR ecosystem growth which supports the development of Australian businesses. CBA welcomes a holistic, cross-government approach to prohibiting screen scraping practices involving customer log-in credentials to access financial data. A clear signal from Government through a formal ban will ensure customers are better protected, and incentivise business to more quickly transition to using safer means, such as the CDR regime. Finally, CBA welcomes the opportunity to participate in pilots with Government agencies to explore the potential in secure data sharing to support business and public policy outcomes.

22. *What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies? What do you consider to be the most serious national security risks presented by critical and emerging technologies, such as AI?*

Accelerating the uptake of critical and emerging technologies, such as AI, will require a whole-of-society effort. Adoption of emerging technologies should be an economic priority for government that will boost productivity and underpin our future prosperity. Data and digital technologies offer incredible potential to reverse productivity decline and strengthen our economic resilience.

Australia must embrace this new era of rapid technological advancement. The change is transformative and Australia risks being left behind as other countries benefit from a new intelligence era. This includes deepening our inference capabilities and driving adoption across the economy, especially among SMBs. In terms of what government can do to advance adoption of AI, CBA would welcome government:

- clarifying its approach to AI regulation and focus its regulatory mandates on growth as an outcome, as well as consumer protection. CBA believes AI regulation should leverage existing regulation, be risk-based, tech neutral and promote innovation.



- helping attract and grow the domestic and global talent pipeline by expanding and fast-tracking skilled visas, improve credential recognition, offering clear pathways to permanent residency for priority tech workers, supporting industry-led upskilling initiatives, and updating school curricula and teacher training in STEM, including industry partnerships.
- encouraging AI adoption across the economy in ways that build trustworthiness, such as grants programs for SMBs to pilot AI tools that improve productivity or providing SMBs with resources to enable experimentation and de-risk adoption.
- role-modelling the use of AI in government to demonstrate benefits and promote public trust, and leverage public procurement to drive adoption, especially among SMBs.

More broadly, Australia's ability to embrace the AI transformation hinges on high-capacity, low-latency connectivity; sovereign, scalable compute; and integrated planning with abundant, reliable, affordable clean energy and infrastructure. Without a national strategy for AI development and adoption, strategic AI infrastructure investments and a smart, balanced approach to regulation in the national interest, Australia risks becoming a wholesale adopter of foreign-owned platforms, with limited control over the underlying systems that shape our digital economy and national security posture.

Realising the benefits of AI requires adoption and community trust. It is important that AI is used safely and ethically. CBA is proud to have contributed to the development of Australia's AI principles, which are a good guide to responsible use of AI. Risks such as synthetic identity fraud, model theft and prompt injection, weaponisation of AI to generate malicious code and automate cyber attacks can have a dramatic and negative impact on trust. A recent global study on trust in AI found half of Australians use AI regularly, but only 36 % are willing to trust it, with 78% concerned about negative outcomes. CBA believes there is role for Government and industry to work together to help enfranchise all Australians in an AI-future, enabling them to take up opportunities offered.

In relation to quantum computing, CBA notes the benefits that could flow from faster data analytics such as enhanced fraud detection, corporate risk simulations and analytics. However, quantum also carries the potential to introduce risks note that cryptographically relevant quantum computer is anticipated to break today's common standard public key encryption methods. CBA welcomes ASD's endorsement of the NIST's Standards on Post Quantum Cryptographic (PQC) algorithms which provide a starting point for organisations to prepare for the when Quantum capability supersedes public key encryption methods. The advice provided by ASD to organisations in relation to planning for a post-quantum environment should be amplified through Horizon 2 of the Cyber Strategy and beyond.[19]

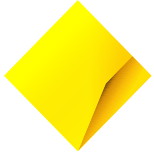
3.3 World-class threat sharing and blocking

23. What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?

24. Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry?

A proactive posture should be built on transparency, shared responsibility, near-real intelligence, and continuous learning. A more proactive cyber security posture should also leverage deeper collaboration between government and industry, particularly in intelligence sharing and incident response. To this end, CBA acknowledges the role of the National Cyber Intel Partnership (NCIP) and believes it best placed to

[19] https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/planning-post-quantum-cryptography



support a more proactive cyber security posture through expanded scope and scaling of near-real time intelligence sharing.

CBA would welcome Government entities providing timely, detailed threat intelligence – including tactics, techniques and procedures and indicators of compromise – to help organisations defend against real-world threats. Joint investigations, shared reporting, and co-authored advisories would also support skills uplift and improve national resilience. Further, CBA would welcome combined Government and industry efforts to bring together shared active cyber defence missions to leverage key talent and capabilities that exist within the private sector, which could aid the Government's proactive cyber posture.

There is also a need for greater clarity around Australia's proactive cyber security posture. There is currently no clear legal framework defining what constitutes permissible Active Cyber Defence (ACD) in Australia which creates uncertainty for organisations that may wish to take more assertive steps to protect their systems.

Government may consider defining a whitelist of acceptable ACD activities – such as deception environments or automated isolation – and establishing safe harbours for approved private-sector participation under government oversight. Clear boundaries would help ensure that defensive actions are lawful, proportionate and coordinated.

25. How could government further support industry to block threats at scale?

Government could play a more active role in helping smaller businesses block cyber threats, particularly those without dedicated cyber, fraud and scams teams.

Federal agencies could assist with takedown requests on behalf of small businesses, by removing malicious branded content on the businesses behalf when a business lacks the technical capability or knowledge to do so. Currently in the financial services context, ASIC is active in this space having taken down more than 14,000 investment scam and phishing websites and continues to remove an average of 130 malicious sites per week.[20] Improving the fidelity of threat indicators and sharing actionable intelligence would also help organisations respond more confidently and effectively.

26. How could the use of safe browsing and deceptive warning pages be amplified?

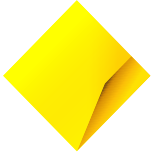
Safe browsing features should be expanded and consistently applied across all platforms, including browsers, mobile apps and connected devices.

Legislation, such as the *Scams Prevention Framework Act 2025,* should enable internet service providers to block access to phishing sites, malware, and other malicious content, similar to existing DNS redirection used for illegal media. Government could also provide APIs for developers to integrate safe browsing checks into their services. Real-time threat intelligence feeds and crowdsourced reporting would help keep deceptive site databases up to date.

Public awareness campaigns should also educate users on recognising browser warnings and understanding the risks of unsafe websites.

27. What more is needed to support a thriving threat sharing ecosystem in Australia? Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?
28. How can we better align and operationalise intelligence sharing for cyber security and scams prevention?

[20] https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2025-releases/25-171mr-scammers-on-notice-as-asic-steps-up-action-to-protect-consumers-from-online-investment-scams/



A thriving threat sharing ecosystem requires stronger incentives and clearer coordination between government and industry. CBA believes building trust and demonstrating the value of shared intelligence will be key to expanding participation.

Some businesses are reluctant to participate in sharing initiatives unless commercial benefits are evident. Low maturity sectors may lack the resources or awareness to engage meaningfully. Government could improve planning and support for Information Sharing and Analysis Centres (ISACs), and work to reduce barriers to entry such as membership costs.

To improve intelligence sharing, government should support platforms like the AFCX Anti-Scams Intelligence Loop and NCIP, which enables actionable data sharing. A universally adopted solution for sharing threat intelligence is currently lacking, which limits the effectiveness of detection and mitigation efforts. Connecting different systems to a central loop and ensuring the data is genuinely actionable would help streamline responses and improve coordination across sectors. It is important that government and private sector capabilities are optimised and the technologies used for intel sharing provide near real-time intelligence, otherwise Australia's threat sharing framework will remain fragmented, incomplete, and slow in response to a heighten and increasingly complex threat landscape.

As the lines between economic crimes (cyber and financial crime, as well as fraud and scams) continue to blur, siloed enforcement efforts mean critical intelligence is lost or under-leveraged. We believe expanding intelligence-sharing capabilities beyond a narrow cyber security lens would unlock economies of scale in detecting and disrupting related harms, while easing the overall resource burden. This includes opportunities to deploy powerful, real-time AI-enabled tools (such as pattern recognition, network analysis and geospatial tracking) through coordinated efforts across industry and enforcement agencies.

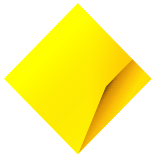
29. *Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?*

Roles and responsibilities in a crisis scenario are not always well understood at the industry-level, and it would be beneficial to clarify the function what each government agency will play in crisis scenarios. Government could improve preparedness and understanding of the role that government agencies play by providing shared scenarios that organisations can use to test their internal and cross-industry responses.

CBA welcomed the National Cyber Exercise Program as part of Horizon 1 of the Cyber Security Strategy, however, believes joint exercises should be expanded in scope and depth, moving beyond desktop-level discussions to full simulations that include government interaction. End-to-end exercises involving multiple sectors would help identify gaps, build muscle memory, and ensure a coordinated national response. To support this, government could develop common scenarios for entities to use internally or across industries, supporting a consistent understanding of potential cyber conflicts and crises. This approach helps compare capabilities, pinpoint areas of overlap and dependence, coordinate responses where needed and enable better cross-industry observation opportunities to support learning and alignment.

30. *How could government better incentivise businesses to adopt vulnerability disclosure policies?*
31. *Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?*

CBA believes the Government can encourage businesses to adopt vulnerability disclosure policies by providing legal protections for individuals and organisations that identify and report vulnerabilities. In most cases, vulnerabilities are discovered by skilled researchers acting in the public interest. Without clear protections, these individuals may face legal action, which discourages responsible disclosure. Establishing



safe reporting mechanisms and shielding researchers from liability would help build a more transparent and secure cyber environment.

CBA would welcome a vulnerability disclosure program should the program feature a strong legal protection for security researchers. Many companies currently pursue legal action against researchers who disclose vulnerabilities, even when done responsibly. Australia already provides some protection under the Copyright Act 1968 (Clause 47H), which allows for reverse engineering, but this should be expanded. Legal safeguards should take precedence over contractual restrictions to ensure researchers can report vulnerabilities without fear of litigation.

The Government has the opportunity to take an active role in establishing vulnerability disclosure programs and bug bounty initiatives within Australia. Similar to practices adopted in the United States, facilitating the publication of program outcomes can help evaluate researcher engagement and measure overall success. For example, the "Hack the Pentagon"[21] initiative launched in 2016 was instrumental in pioneering government-led bug bounty programs, and numerous agencies now utilise platforms to efficiently manage security reports. While vulnerability disclosure programs do not necessarily require monetary compensation for hackers, providing rewards has consistently demonstrated its effectiveness in motivating broader participation.

3.4 Protected critical infrastructure

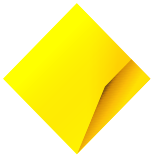
32. *How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?*
33. *Are there significant cyber security risks that are not adequately addressed under the current framework?*
34. *Is the regulatory burden on industry proportionate to the risk and outcomes being sought?*

The SOCI Act has made significant progress in strengthening Australia's cyber resilience, particularly through its expansion to cover telecommunications and the introduction of Enhanced Cyber Security Obligations.

However, the legislation remains complex and difficult to interpret, especially for smaller organisations. There is confusion at the industry-level around which obligations apply to which sectors, and overlaps with other frameworks like CPS 234 can add to the regulatory burden. CBA believes the next phase of the strategy should focus on simplifying these obligations and ensuring they are enforceable. Additionally, recovery capability should be prioritised alongside prevention, recognising that even well-defended assets may be compromised.

The SOCI Act and APRA's CPS 230 both address third party risk, with CPS 230 providing a broader framework for managing these risks, including fourth party risk, and extending to various service providers beyond traditional suppliers. CPS 230 acknowledges ongoing risks associated with the use of third parties across organisations. In comparison, the SOCI Act primarily focuses on outcomes related to notification obligations, without detailed provisions for managing risk. Greater alignment or clarification between these frameworks could facilitate more consistent management of third-party risks within critical sectors. CBA would welcome alignment with the CPS 230 to better ensure the protection and resilience of critical infrastructure assets.[22]

[21] https://www.defense.gov/News/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/
[22] https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf



Overall, CBA believes the regulatory burden commensurate to risk and outcomes being sought is proportionate. CBA strongly welcomes the approach taken by the Cyber and Infrastructure Security Centre (CISC) whereby should obligations from other regulators already exist, CISC has allowed exemptions from duplicative SOCI requirements. However, there is a broader opportunity to ensure that regulation supports both security and innovation. As Australia focuses on productivity and growth, cyber regulation should be designed to enable safe innovation, not just compliance.

35. *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?*

While there is extensive guidance on preventing cyber incidents, CBA observes that there is less support for recovery and resilience.

Government could help by developing resources that focus on organisational recovery – not just technical incident response. Sector-level initiatives, such as cross-industry exercises, help build muscle memory and identify gaps in resilience and could be enhanced by a detailed breakdown of lessons learnt and future actions taken to build resilience. Government support in consolidating roles and responsibilities, improving coordination plans, and facilitating public communications would strengthen industry-wide preparedness.

CBA has invited Government representatives and regulators into observe internal cyber exercises and would welcome further discussions in the development of Horizon 2 on how to best optimise cyber exercises in light of the evolving threat landscape.

36. *How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?*
37. *How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?*

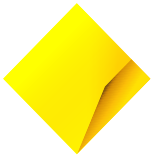
Government can support private sector partners by providing clearer and more up-to-date guidance on which vendors and products meet security expectations. This includes identifying sovereign alternatives and clarifying which suppliers pose higher risks.

Simplifying third-party risk management—such as vetting the US System and Organisation Controls 2 controls for Australian suitability—would further reduce the burden on businesses. Sponsoring certification events, offering incentives for upskilling, and publishing trusted training pathways would assist private sector partners engage more effectively with government requirements and lift economy-wide cyber resilience.

Government frameworks such as CPS 234 are being adopted by private sector partners as a roadmap for strengthening cyber maturity. These frameworks help organisations improve risk management and operational controls and support continuous improvement through regular assessments. By aligning with these standards, businesses can build resilience and maintain customer trust while meeting evolving security expectations.

3.5 Sovereign Capabilities

38. *What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?*
39. *What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?*



40. *What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?*

Government should take a leadership role in building a cyber workforce that is diverse, future-ready and resilient. CBA would welcome the establishment of a National AI and Cyber Vocational Centre to deliver accessible, adaptive education across AI and cyber disciplines.

Rather than focusing solely on 'cyber workers', strategies developed through Horizon 2 should consider broader market segments – such as software engineers and product managers – who contribute to cyber outcomes. Initiatives should include universal access to learning tools, rapid-response training aligned with emerging technologies, and streamlined migration pathways for global talent. Co-investment models and inclusive policies will help ensure all Australians benefit from workforce development.

Successful programs from which the Australian Government can draw from include the NSW Digital Skills and Workforce Compact, which aims to fill 20 % of entry-level digital roles via alternative pathways. CBA's Career Comeback Program, EmpowHer sponsorship initiative, and Tech Associates Program have supported career changers and women in tech and provide additional examples of workforce transition pathways.

Partnerships with Year13 and Telstra have helped raise awareness among young people. International efforts, such as Microsoft's AI Digital Skills Initiative and #10kWomen program in New Zealand, also offer valuable models. These initiatives demonstrate the importance of flexible entry points, targeted support, and inclusive outreach in building a diverse cyber workforce.

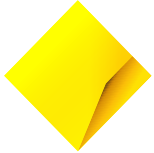
Industries such as defence and transport and logistics offer highly transferrable skills for the cyber workforce. These sectors bring strengths in problem solving, critical thinking, and communication – skills that are essential in cyber roles. Operational technology experience in logistics also aligns well with critical infrastructure needs. Career changers from these industries have already shown success in transitioning into cyber roles.

41. *How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals?*
42. *How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities?*
43. *How would we best identify and prioritise sovereign capabilities for growth and development across government and industry*

Australia's security environment is increasingly contested and complex. Amid rising uncertainty and geopolitical shifts, a confident vision for growth should include efforts to protect Australia's economic and social interests, including safeguarding sovereign capability in critical sectors, such as cyber security.

As noted in response to question 1, CBA believes Australia should define, identify, and develop sovereign cyber capabilities to as part of a broader whole-of-nation approach to economic resilience that embeds the role of business. A clear set of defined sovereign capabilities in relation to cyber security and a shared understand on the outcomes sought between government, industry, and Australia's research community will focus efforts to build capability and channel capital into priority areas. There is a role for Government, with input drawn from industry, to set out what Australia's sovereign cyber capabilities are, longer term definitions and ongoing measurement of those capabilities. CBA believes there is an ongoing role for the Executive Cyber Council in this regard.

Once defined and identified, collaboration across sectors should be anchored in a clear set of sovereign cyber capabilities. Currently, terms like "sovereign capability" and "skills uplift" are too broad to guide



meaningful action. Once specific goals are defined, government agencies can better coordinate policies and industry development initiatives and resources deployed into Australia's research institutions can align to strategic needs which will have the greatest impact.

CBA notes the work of Government that is being progressed via the Universities Accord to deliver new knowledge, innovation and capability and closer collaboration with industry[23]. Clear strategic priorities would allow universities, the research sector, and industry to align and prioritise efforts to develop capability. By identifying national focus areas such as quantum cryptography or sovereign cloud capability, government can guide collaborative planning between research and industry to that capability is being prioritised where it is needed.

44. What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?

While Australia should have a clearer picture of where it needs to build sovereign cyber capability, Government and industry alike need to understand key areas of ICT concentration to inform mitigation strategies to reduce the impact of over-reliance on these technologies.

Australia's digital ecosystem heavily depends on a few foreign technology providers. Cloud and data infrastructure is largely controlled by multinational firms, raising sovereignty and security issues. Telecommunications networks also face concentration risks – until recently, a single foreign vendor could dominate 5G equipment, posing supply and security vulnerabilities. Australia also relies entirely on imports for critical IT components, such as semi-conductors. This import-dependence leaves the nation exposed to global supply shocks or export controls on technology.

Adopting multi-cloud and multi-vendor strategies (both in government and industry procurement) spreads risk and avoids single points of failure. Government policies should integrate concentration risk assessments into cyber security and infrastructure planning – for example, requiring agencies to have contingency plans if one provider fails. Ongoing collaboration with security agencies can help manage foreign interference risks in supply chains, ensuring vendors and imports are vetted for geopolitical risk.

Strengthening domestic tech capability is equally crucial. This includes investing in local R&D and startup ecosystems for cloud and cyber security and leveraging partnerships with trusted allies for technologies Australia cannot build alone.

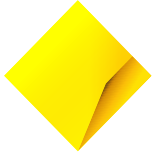
3.6 Strong region and global leadership

45. In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?
46. What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?

Australia should focus on shaping global cyber norms through active participation in the UN Working Group and implementation of the UN Cybercrime Convention. These forums provide opportunities to promote an open and secure internet. As international frameworks on AI begin to take shape, Australia should also seek to play a leadership position in international forums which seek to shape global standards, rules, and governance of how AI is developed and deployed.

Regionally, expanding programs like Southeast Asia Pacific Cyber Program (SEAPAC) and continue to monitor the success of Cyber RAPID, which is still in its infancy, will strengthen resilience and reinforce

[23] https://ministers.education.gov.au/clare/universities-accord



Australia's leadership. Australia should also engage in international standards bodies and align domestic initiatives –such as smart device security and operational technology controls – with global frameworks. Continued leadership in the Counter Ransomware Initiative and related coalitions will help link domestic reporting obligations to global disruption efforts.

Australia should prioritise alignment with major international frameworks, including:

- the EU's Digital Operational Resilience Act which target ICT risks and introduces clear rules for ICT risk management, incident reporting, operational resilience testing, and oversight of ICT third-party risks
- the UK's Product Security and Telecommunications Infrastructure Act for smart device security which requires manufacturers of UK consumer connectable products (or 'smart' products) to comply with the relevant obligations set out in the Act.
- US regulations such as Cyber Incident Reporting for Critical Infrastructure Act requiring critical infrastructure entities to report certain cyber incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency and SEC cyber disclosure rules.
- Singapore's Monetary Authority of Singapore TRM Guidelines that offer a strong model for operational resilience in financial services.

Harmonising with these frameworks would reduce compliance complexity, support cross-border trade, and position Australia as a leader in secure digital markets.