FinTech Australia

[redacted]

29 August 2025

Department of Home Affairs
6 Chan Street
Belconnen ACT 2617

Submitted electronically

FinTech Australia Submission to Horizon 2 of the 2026-2030 Australian Cyber Security Strategy

FinTech Australia welcomes the opportunity to provide a submission on the discussion paper on Horizon 2 of the 2026-2030 Australian Cyber Security Strategy (**Discussion Paper**).

About FinTech Australia

FinTech Australia is the peak industry body representing the Australian fintech sector, with a membership of more than 400 companies and startups nationwide. Our members span the full breadth of the fintech ecosystem, including payments, consumer and business lending, artificial intelligence, wealthtech, regtech, neobanking, open banking, cryptocurrency, blockchain, DeFi, and Web3. The fintech industry delivers a wide range of business-to-business and business-to-consumer financial products and services that support the smooth operation of the Australian economy.

Our vision is to position Australia as one of the world's leading markets for fintech innovation and investment. This submission has been compiled by FinTech Australia and its members in an effort to advance public debate and drive cultural, policy and regulatory change toward realising this vision, for the benefit of the Australian public.

Introduction

Australia's fintech sector sits at the front line of cyber risk and cyber resilience. We consider that Horizon 2 should lock in three simple outcomes: (1) make it easier and cheaper for small entities to do the basics; (2) scale what already works (threat blocking, intel sharing, incident learning) across the whole economy; and (3) align the fast-moving rules for data, privacy, scams and software security so businesses can invest with certainty.

We welcome the Government's progress under Horizon 1 and support an ambitious, industry-shaped program for Horizon 2. Our response below follows the 50 consultation questions in the Discussion Paper.

Responses to consultation questions

2. Developing our vision for Horizon 2

Q1. 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?
Emerging trends likely to shape the cyber security outlook over the next few years include the growing use of artificial intelligence and machine learning in both cyber defence and attacks, the rapid adoption of quantum-resistant encryption, and the continued digitisation of financial services across borders.

From a fintech perspective, the expansion of open data frameworks such as the Consumer Data Right will create new opportunities for secure data sharing. At the same time, growth in decentralised finance and tokenised assets will test existing regulatory and supervisory approaches, making interoperability and aligned standards critical.

Other strategic factors the Government should consider under Horizon 2 include ensuring cloud resilience given increasing reliance on third-party providers, investing in skills and talent pipelines for both fintech and cyber professionals, and embedding stronger international cooperation on cross-border payment security, data flows and scam prevention. By focusing on these areas, Australia can strengthen trust in digital financial infrastructure, support fintech innovation, and maintain alignment with global best practice in cyber security.

Q2. Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?
FinTech Australia does not have a specific comment to provide in response to this question.

Q3. Does the high-level Model resonate and do you have any suggestions for its refinement?
FinTech Australia does not have a specific comment to provide in response to this question.

Q4. Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?
FinTech Australia does not have a specific comment to provide in response to this question.

3.1 Shield 1: Strong businesses and citizens

Q5. What could government do to better target and consolidate its cyber awareness message?
The government's cyber awareness messaging would have greater impact if it was more consistent, practical and tailored to different audiences, including fintechs and their customers. At present, messaging often comes from multiple agencies with overlapping campaigns, which can create confusion and dilute trust. A more effective model would consolidate messaging through a single, clearly recognised government voice that works in partnership with industry to co-design content.

Q6. 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?
FinTech Australia does not have a specific comment to provide in response to this question.

Q7. How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?
The Government could encourage greater uptake of existing cyber resources by making them more visible, practical and easy to integrate into day-to-day operations. Some small businesses and NFPs are aware that cyber is important but unaware where to start or assume the resources are too complex or costly to adopt.

Q8. How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?
FinTech Australia does not have a specific comment to provide in response to this question.

Q9. What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFPs?
FinTech Australia does not have a specific comment to provide in response to this question.

Q10. 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?
FinTech Australia does not have a specific comment to provide in response to this question.

Q11. 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?
FinTech Australia does not have a specific comment to provide in response to this question.

Q12. How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?
The threat of ransomware is well understood in broad terms, but its practical impact on individuals and small entities is often underestimated. For these groups, ransomware isn't just about data theft, it can completely halt day-to-day operations, cut off access to critical records, and in many cases threaten the financial viability of the organisation.

A key issue for small entities is the preparation of response plans for cybersecurity contingencies and finding the time and resources to effectively prepare, test and update them. This is an important area in which further government support would confer a practical benefit.

Q13. How could the government further support businesses and individuals to protect themselves from ransomware attacks?
The government could play a stronger role in helping businesses and individuals protect themselves from ransomware by focusing on prevention, response and awareness. For prevention, support could be given through free or subsidised cyber health checks, simple guidance tailored to different industries, and promoting regular practices such as backups and patching.

On the response side, a national hotline and rapid-response service could give victims a clear pathway to report incidents and access immediate help, backed by a government-supported recovery fund or cost-sharing scheme for smaller organisations.

Awareness is equally important, with broad public education campaigns, sector-based information sharing, and closer coordination with insurers to make cyber insurance more transparent and affordable.

Q14. 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?
FinTech Australia does not have a specific comment to provide in response to this question.

Q15. How can support services for victims of identity crime be designed to be more effective in the context of increasing demand?
FinTech Australia does not have a specific comment to provide in response to this question.

Q16. Which regulations do you consider most important in reducing overall cyber risk in Australia?
The most important regulations for reducing cyber risk in Australia are those that establish clear, enforceable standards and improve accountability across sectors.

The Privacy Act as well as penalties for its violation and the potential for civil compensation claims - especially in relation to Australian Privacy Principle 11 and data breach notification requirements - are central, as they incentivise organisations to invest in stronger security and be transparent when incidents occur.

The Security of Critical Infrastructure Act (SOCI Act) is also vital, as it compels operators of essential services to maintain robust protections and report cyber incidents. Prudential standards like APRA's CPS 234 play a major role in ensuring financial institutions manage cyber risk to a high and consistent baseline.

For fintechs, it is important to see more proportionate application of those regulatory obligations through the supply chain. These regulations have a huge impact for suppliers to APRA regulated entities as a result of contractual pass through of compliance obligations. This can often occur without detailed risk assessment being undertaken by APRA regulated entities. The result is that competition and innovation are reduced, because many fintechs are either shut out of supplying to these entities or need to absorb increased compliance costs.

Q17. Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?
Fintechs often face overlapping and inconsistent requirements across privacy, scams, SOCI Act and sector rules, which results in duplicative assessments. A single reporting portal with aligned definitions and timeframes would reduce cost and keep attention on genuine risk. The introduction of a consistent baseline approach to due diligence would be welcome to many fintechs.

3.2 Shield 2: Safe technology

Q18. 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?
FinTech Australia does not have a specific comment to provide in response to this question.

Q19. 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?
FinTech Australia does not have a specific comment to provide in response to this question.

Q20. What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?
FinTech Australia does not have a specific comment to provide in response to this question.

Q21. 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?
FinTech Australia does not have a specific comment to provide in response to this question.

Q22. 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?
FinTech Australia does not have a specific comment to provide in response to this question.

Q23. What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies?
FinTech Australia does not have a specific comment to provide in response to this question.

3.3 Shield 3: World-class threat sharing and blocking

Q24. 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?
Screen scraping and the Consumer Data Right

Many members of FinTech Australia are supportive of a ban on the use of screenscraping to collect banking data. This is due to cybersecurity concerns and an appetite to see banking data instead be collected under the more secure Consumer Data Right framework.[1]

The Consumer Data Right

The Consumer Data Right uses a secure accreditation and consent-based authorisation model developed by Treasury to facilitate the secure exchange of data. Under the Consumer Data Right, once a consumer provides their consent, the consumer's banking data is transmitted by their bank to a third party which has been accredited by the ACCC. There are strict obligations imposed by law on the accredited data recipient, for example placing limitations on how they may use data obtained through the Consumer Data Right.

The Consumer Data Right offers significantly better cybersecurity than alternatives such as screen scraping, while offering much better user experience than manual data entry. The Consumer Data Right has been rolled out to the banking and energy sectors, and further expansion to sectors such as non-bank lending is underway.

[1] Screen scraping refers to technology (known as digital data capture) which collects (scrapes) data displayed on a screen.

Where the Consumer Data Right is available as a viable alternative, FinTech Australia supports a Government-led transition away from screen scraping and towards the Consumer Data Right.

Problems with screen scraping for banking data

Currently, the matter of most concern to us is that consumers are often asked to share their banking login details to enable a third party to collect their banking data through screen scraping, either on a one-off or ongoing basis. This application of screen scraping represents a major cybersecurity weakness in the data economy.

The risks of screen scraping have been raised in at least six major consultations over the past eight years.[2] Risks of using screen scraping in banking include that it:

- constitutes a systemic cybersecurity risk;
- undermines banks' fraud protection controls;
- normalises poor cybersecurity hygiene by consumers;
- mat put consumers in violation of their banks' terms of service, potentially adversely impacting their eligibility for compensation in the event of a data breach; and
- creates related privacy risks. For example, it does not strictly comply with the data minimisation principle, that data should only be collected where it is actually necessary.

It is important to note, however, that to date that FinTech Australia is not aware of any evidence of screen scraping leading to a banking data breach.

In the course of a 2023 Treasury consultation on banning screen scraping,[3] a wide range of stakeholders expressed in-principle support for banning the use of screen scraping, generally where viable alternatives exist, including the:

- Financial Services Council;
- Australian Banking Association;
- Law Council;
- ACCC;
- ASIC;
- Consumer Action Law Centre;
- Financial Rights Legal Centre;
- Office of the Australian Information Commissioner; and
- Commonwealth Bank of Australia.

Additionally, FinTech Australia considers that the present availability of screen scraping for banking data collection represents a deterrent to the adoption of the Consumer Data Right. This is because there is a reduced incentive to use the Consumer Data Right and comply with its high regulatory standards when firms can instead resort to screen scraping and bypass these obligations. By phasing out screen scraping, the Government can therefore both enhance the cyber resilience of Australia's financial system while also addressing a current Treasury policy objective of improving the adoption of the Consumer Data Right in banking. Importantly,

[2] Treasury consultation on screen scraping (2023), Privacy Act Review (2023), Statutory Review of the CDR by Elizabeth Kelly (2022), inquiry by the Senate Select Committee on Financial Technology and Regulatory Technology (2019-21), Inquiry into Future Directions for the Consumer Data Right (2020) and Review into Open Banking in Australia (2017).

[3] Treasury, Screen scraping – policy and regulatory implications (2023).

however, the Consumer Data Right needs to provide an equivalent option for businesses and consumers, including from a compliance and user experience perspective.

Conclusion

FinTech Australia recognises that screen scraping presently plays an important role in the financial services industry, but also notes where a viable alternative exists - such as the Consumer Data Right for banking data - there are strong public policy grounds for banning screen scraping.

FinTech Australia considers that in the event the use of screen scraping for banking data is banned, it is important that a smooth transition can occur by setting a clear timeline for phasing out its use.

Other

Separately and in addition to the above, FinTech Australia considers that the Government should encourage lawful active-defence practices: automated blocking using community-shared indicators, takedown requests, defences against credential-stuffing, and the use of honey-tokens to detect misuse. Clear guidance and simple integrations will help small firms participate.

Q25. Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry?
Yes, publish plain-English guidance that sets out permissible techniques, escalation steps and evidence handling, with a safe harbour when organisations act in line with that guidance. This will give confidence to act quickly.

Q26. How could government further support industry to block threats at scale?
FinTech Australia does not have a specific comment to provide in response to this question.

Q27. How could the use of safe browsing and deceptive warning pages be amplified?
Through working with major browsers and banks to standardise the language on deceptive-site warnings and link users to immediate next steps, freeze accounts and lodge a report.

Q28. 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?
Please refer to our answer to question 24.

Q29. How can we better align and operationalise intelligence sharing for cyber security and scams prevention?
Build a joint operating picture that links cyber indicators with mule-account patterns and scam typologies, and establish fast channels to push blocks across banks and platforms. This is where cyber and scams prevention meet.

Q30. 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?
FinTech Australia does not have a specific comment to provide in response to this question.

Q31. How could government better incentivise businesses to adopt vulnerability disclosure policies?
Offer a standard vulnerability disclosure policy template and a small grant or fee rebate for SMBs that implement it, and recognise adoption in procurement and insurance. This brings researchers and small firms together safely.

Q32. Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?
FinTech Australia does not have a specific comment to provide in response to this question.

3.4 Shield 4: Protected critical infrastructure

Q33. How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?
The SOCI Act sets a strong foundation for protecting critical infrastructure, but its effectiveness varies across sectors. While obligations are proportionate in principle, fintechs and smaller players often face overlap with existing requirements (e.g. CPS 234, AUSTRAC), creating compliance burden without clear additional benefit. Greater clarity, sector-specific guidance and coordination across regulators would improve understanding and ensure obligations are consistently enforceable.

Q34. Are there significant cyber security risks that are not adequately addressed under the current framework?
Please refer to our answer to question 24. In addition, while the SOCI Act addresses core infrastructure risks, there remain gaps. In particular, the framework does not adequately cover supply chain vulnerabilities, third-party service providers (such as cloud and payments infrastructure), and the specific risks fintechs face from reliance on screen scraping. The Act also focuses heavily on large entities, leaving smaller but interconnected operators exposed. Stronger coordination across sectors, clearer incident reporting channels, and targeted guidance for emerging technologies would help address these risks.

Q35. Is the regulatory burden on industry proportionate to the risk and outcomes being sought?
The regulatory burden under the SOCI Act is not always proportionate to the risks or outcomes being sought. Larger, well-resourced institutions are generally able to absorb the cost of compliance, but smaller players and innovative fintechs often face the same obligations without the same capacity. This creates a disproportionate burden that can stifle competition and innovation, without necessarily improving overall security outcomes.

Q36. 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?
Critical infrastructure owners and operators would benefit from practical, outcomes-focused support rather than additional layers of prescriptive compliance. Many entities, particularly smaller operators and new entrants, struggle not with awareness but with the cost and complexity of implementing uplift.

Government could play a stronger enabling role by:

- Providing accessible tools and frameworks tailored to sector-specific risks, with clear guidance on what "good" looks like for different sizes and types of organisations.
- Offering financial incentives such as grants, co-funding or tax offsets to encourage uplift, especially where investment in cyber resilience does not directly generate revenue.
- Facilitating timely information-sharing between government, regulators and industry to ensure emerging threats are widely understood and can be responded to quickly.
- Supporting skills development programs to address workforce shortages in cyber security and operational resilience.

Q37. How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?
The private sector often finds government security requirements complex, fragmented across agencies, and costly to implement. To improve engagement and compliance, government could:

- Simplify and harmonise requirements: Streamline security certifications and technical controls to avoid duplication across frameworks (e.g. ISM, PSPF, DISP, and international standards).
- Provide clear and consistent guidance: Offer plain-language resources and worked examples that translate security requirements into practical steps for different types of businesses.
- Support scalable pathways: Develop tiered or proportional certification models so that smaller operators can demonstrate compliance without the overhead faced by large corporates.
- Offer technical assistance and tools: Provide templates, automated tools, and pre-approved solutions that lower the cost and complexity of meeting requirements.
- Create incentives for early adoption: Consider grants, tax offsets, or procurement preferences for firms that invest in security certification and uplift.
- Engage in two-way consultation: Maintain regular dialogue with industry so that requirements remain fit-for-purpose, risk-based, and do not inadvertently exclude innovative providers.

Q38. How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?
Australian Government security requirements and frameworks are increasingly being adopted by the private sector, particularly in areas tied to critical infrastructure and regulated industries.

For example, uptake via data regimes: frameworks such as the Consumer Data Right and Digital ID system have embedded government-level security requirements (e.g. strong encryption, consent management, authentication). These have set a benchmark for fintechs and technology providers that often exceeds baseline commercial practice.

3.5 Shield 5: Sovereign capabilities

Q39. 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?
FinTech Australia does not have a specific comment to provide in response to this question.

Q40. 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?
FinTech Australia does not have a specific comment to provide in response to this question.

Q41. 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?
Prioritise people from network operations, software engineering, data analysis, audit and compliance. Short bridging courses and employer incentives for on-the-job training can convert these skills quickly.

Q42. 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?
Co-design a fintech cyber research agenda around secure payments, AI for fraud detection and privacy-preserving analytics, with matched funding and open testbeds that startups can access.

Q43. How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities?
FinTech Australia does not have a specific comment to provide in response to this question.

Q44. How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?
Focus on areas where Australia already shows strength such as payments security, digital identity, cryptography, secure software supply chains and incident-response tooling and build depth through procurement and research support.

Q45. What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?
FinTech Australia does not have a specific comment to provide in response to this question.

3.6 Shield 6: Strong region and global leadership

Q46. Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?
FinTech Australia does not have a specific comment to provide in response to this question.

Q47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?
Australia has an important role to play in shaping cyber security capability in Southeast Asia and the Pacific, but this should be done in a way that is practical, collaborative and recognises the different levels of maturity across the region. From a fintech perspective, there is an opportunity to share lessons learned from implementing frameworks such as the Consumer Data Right and payments system reforms, which balance innovation with strong security safeguards. This type of knowledge transfer could help neighbouring markets develop interoperable systems that both enhance consumer protection and enable cross-border financial services.

Q48. Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?
FinTech Australia does not have a specific comment to provide in response to this question.

Q49. 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?
In Horizon 2, Australia should concentrate its efforts in forums where the intersection of digital economy, financial services, and cyber security is shaping regional and global norms.

For instance, Australia's priorities should include promoting secure cross-border data flows, ensuring interoperability of digital identity frameworks, and embedding strong but flexible cyber security standards that can be adopted by fast-moving industries like fintech.

Q50. What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?
For Australia's efforts on international cyber regulatory alignment, priority should be given to frameworks that directly affect financial services and the fintech sector, where cross-border operations are common and regulatory fragmentation creates unnecessary friction. Alignment with international standards on digital identity, data protection, and payments security should be central, given their direct impact on fintech trust, adoption, and competitiveness.

Of particular importance is international consistency in open banking and open data regimes. Australia's Consumer Data Right can be a source of influence in shaping global frameworks. Aligning data-sharing, consent, and security requirements would reduce compliance duplication for fintechs operating regionally and globally.

Finally, cyber risk management for digital assets and stablecoins should be considered a frontier area for alignment. With multiple jurisdictions developing frameworks, Australia's involvement will ensure our standards reflect both security and innovation, while supporting safe participation in global financial markets.

Next Steps

FinTech Australia appreciates the opportunity to contribute to this consultation and looks forward to continued engagement with the Department of Home Affairs. We would welcome the opportunity to meet with you or your team to discuss cybersecurity issues in more detail and explore how we can work together to improve Australia's resilience to cybersecurity threats.

[redacted]

Yours sincerely

[redacted]
Fintech Australia