To: Department of Home Affairs,
Cybersecurity Horizon Two,
Cyber Security Strategy Program Management Office,
By email: CSSH2@homeaffairs.gov.au

5 September 2025,

Dear Cyber Security Strategy team,

The Digital Industry Group Inc. (DIGI) thanks the Department of Home Affairs for the opportunity to provide feedback on the *Charting New Horizons: Horizon 2 Cyber Security Strategy Discussion Paper* (the Discussion Paper).

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, Discord, eBay, Google, HelloFresh, Meta, Microsoft, Pinterest, Snap, Spotify, TikTok, Twitch and Yahoo. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

DIGI shares the Government's strong commitment to cyber security, and our members invest heavily in cyber and data security and the privacy of their users, through technical controls, user controls and strong accountability-based practices and policies.

DIGI recognises the role that large-scale data breaches in the telecommunications, aviation, and insurance sectors in recent years have played in underscoring the critical importance of data privacy and cyber security economy-wide, and the serious impact that any such event can have on Australians. To that end, we applaud the Government's ambition to build a world-leading cyber security ecosystem by 2030, as outlined in the *2023–2030 Australian Cyber Security Strategy*.

In addition to the submission below, we encourage consideration of our previous submissions in relation to wider initiatives that mitigate against cyber security threats, including non-regulatory and cyber security consumer awareness and targeted industry initiatives.

We thank you for the opportunity to contribute to the Horizon 2 consultation and to share industry perspectives on strengthening collaboration, reducing regulatory complexity, and scaling cyber security maturity across the economy. We look forward to future opportunities to continue our engagement. Should you have any questions, please do not hesitate to contact my colleague [redacted] via [redacted]

Best regards,

[redacted]

[redacted]

Table of contents

DIGI supports continued focus on building cybersecurity capability

1. Reflections on Horizon 1

1.1. DIGI commends the progress achieved under Horizon 1, particularly in improving cyber incident coordination, appointing the National Cybersecurity Coordinator, elevating baseline security, and embedding cyber security messaging across communities.

1.2. We note that many of the schemes proposed in Horizon One (security standards for consumer-grade smart devices, voluntary, industry-led labelling scheme for consumer-grade smart devices) are in various stages of progression. We refer to DIGI's submission to the 2024 *2023–2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper* for more detail on DIGI's position on the best path to progress these schemes.

1.3. Horizon 2 represents a critical opportunity to consider how Australia:

1.3.1. Scales capability, awareness and education initiatives across Australian consumers and small businesses.

1.3.2. Builds agile, interoperable regulatory settings that align with global standards.

1.3.3. Strengthens international cooperation on cyber resilience and threat disruption.

1.4. DIGI support the goals stated in the Discussion Paper to:

Embed cyber security messaging, standards, capability and efforts across society, from our homes and schools to our businesses and government partners;

Empower business (particularly small business), not-for-profits and citizens to protect ourselves and each other, reducing the barrier for applying protective frameworks ensuring

Australian businesses are more productive and bounce back quicker; and

Enhance our cyber regulatory frameworks through structural reforms to harmonise and simplify regulation, strengthen our cyber workforce.

1.5. We strongly support the Government's whole-of-economy, partnership based approach and urge continued collaboration with industry in designing policies, standards, and guidance materials.

2. Building cyber security literacy across Australia

2.1. There is a shared responsibility to address cyber security risks across governments, industry, and the broader community. It is in the interest of companies to take action to ensure strong cyber security and DIGI members invest heavily in the cyber security of their services.

2.2. DIGI has long supported education initiatives that uplift capability and encourage strong cybersecurity practices for businesses, organisations and individuals. Cyber security interventions must remain responsive to an evolving threat landscape. Education and awareness initiatives are a key lever to maintain flexibility in Australia's cybersecurity response and complement technical requirements.

2.3. DIGI supports the consolidation of consistent cyber safety messaging across the economy. Awareness initiatives, such as Act Now. Stay Secure., contain action-oriented educational materials to uplift the baseline consumer knowledge of cybersecurity best practices. We support cyber security messaging that shares practical, real-world behaviours for individuals and small businesses such as using two-factor authentication, choosing strong unique passwords, and keeping up to date with software updates. These simple behaviours can make a tangible difference for cybersecurity outcomes and consistent education is key to driving this messaging across relevant groups.

2.4. The Government should continue leveraging evidence-based approaches and co-design campaigns with industry and community organisations to maximise reach and effectiveness. We have previously expressed our support for close collaboration between industry and government and there is a continued willingness among industry to build capability and best practice economy-wide.

2.5. In previous submissions, DIGI has stressed that secure-by-design principles must complement, not replace, cyber security best practices and behaviours for all, including consumers. DIGI has previously cautioned that industry interventions or approaches should be complemented by continual education, training and vigilance, to avoid fostering a false sense of security for consumers.

2.5.1. For example, DIGI recognises that the Australian Government has awarded the grant to co-design and implement an industry-led and internationally aligned voluntary labelling scheme for consumer-grade smart devices in Australia and this work is currently underway.[1]

[1] https://business.gov.au/grants-and-programs/labelling-scheme-for-smart-devices

2.5.2. In previous submissions, DIGI has cited a position paper titled *Cyber Security Labelling: A Guide for Policymakers,* in which the ITI advances several points that highlight the need to continually deliver consumer education initiatives, in addition to industry led security practices.[2] In this paper, ITI states: '*Manufacturers can build the strongest capabilities into a device or service, but the likelihood that device or service is compromised by a cyber-attacks increases if end-users or operators do not undertake appropriate precautions*'. This sentiment is consistent with the experiences of DIGI members, and we agree with ITI's view that initiatives, such as labelling, 'should not convey a false sense of security' and such initiatives must always be complemented with continual education regarding cybersecurity best practices.

Clarity, coherence and reducing regulatory complexity

3. Data protection and minimisation

3.1. DIGI recommends that reforms under Horizon 2 continue to consider the interrelation of cyber security and privacy frameworks, including efforts to harmonise and simplify regulation to drive compliance. DIGI has supported increased mandatory cyber security and related obligations in the reform of the Privacy Act, in order to level up controls and processes within all entities subject to that Act, noting clarity is essential to avoid unnecessary duplication and regulatory complexity.

3.2. In DIGI's submission to the *2023-2030 Australian Cyber Security Strategy Discussion Paper*, we supported a thorough gap analysis to inform the best approach to improve incident response[3]and we welcome the Government's signalled approach in continuing to address areas of regulatory overlap, in order to reduce complexity and strengthen outcomes. In line with DIGI's support for overall clarity in the regulatory regime related to cyber security, we support and encourage the Department of Home Affairs' continued engagement with the Attorney-General's department on the direction of privacy reform.

3.3. There are notable areas of overlap between government responses to cyber security and privacy, such as in the regulation of data storage practices that, without clear consideration and guidance, could prove complex for industry to navigate and pose barriers to compliance. We equally recognise that there is an opportunity for increased mandatory cyber security and related obligations in the ongoing reform of the Privacy Act that could result in a more coordinated approach and stronger cyber security outcomes. We note, for example, that the Government's response to the *Privacy Act Review Report* agreed in-principle that entities should be required to comply with a set of baseline privacy outcomes, aligned with relevant outcomes of the *Government's 2023–2030 Australian Cyber Security Strategy* (proposal 21.2). DIGI has welcomed the inclusion of cyber security measures within the APPs. For example, DIGI has long advocated for the importance of data minimisation, as the more information that is required to be collected

[2] ITI, (April 2021), cyber security Labelling: A Guide for Policymakers

[3] DIGI submission to *2023-2030 Australian Cyber Security Strategy Discussion Paper*, Accessed at: https://www.homeaffairs.gov.au/reports-and-pubs/PDFs/2023-2030-aus-cyber-security-strategy-discussion-paper/DIGI-submission.PDF

and retained by companies can increase the severity of a potential breach.

3.4. Data minimisation requires goods or service providers to not seek to collect data beyond what is reasonably needed to provide the good or service, or to employ adequate measures to anonymise data. We believe that privacy risks – such as inappropriate use or disclosure or poor security – can be reduced by resolving the tension between data retention requirements and data minimisation best practices. DIGI welcomes the fact that the universally accepted privacy best practice of data minimisation forms part of the existing APPs under the Privacy Act 1988 (Cth). This principle equally serves privacy and cyber security outcomes.

3.5. We encourage continued engagement to map potential areas of overlap in tranche two of the Government's ongoing privacy reform. The Government response to the *Privacy Act Review report* was released in 2023 however, the full scope and legislative timeframe for 'tranche two' of the reform of the Privacy Act remains unknown. The lack of clarity on the scope and timeframe for remaining reforms creates uncertain conditions for businesses and consumers, including in the relevant overlap with cybersecurity obligations. Clarity for consumers over protections under both the privacy and cybersecurity regimes could also boost trust and confidence in the use and uptake of digital technologies.

3.6. To ensure that cyber security and privacy regimes are cohesive, we support the continued provision of appropriate guidance material to assist industry in understanding the relevant set of obligations and regulating authority related to different practices, and the intent to manage the burden on industry of overlapping consultation processes by coordinating consultation on cybersecurity and privacy reforms. This will help achieve a response with clear obligations for industry that focus on cyber security outcomes without creating unnecessary regulatory burden or reporting procedures that are complex to navigate and that have the potential to conflict.

4. Scams and identity theft

4.1. DIGI is committed to the Government's mission to make Australia a harder target for scammers. We acknowledge the connections between criminal scam activity and identity theft, however we consider unauthorised fraud, such as cybercrimes that may use hacking, data breaches and identity theft, that do not involve the deception of a consumer into 'authorising' the fraud, as distinct categories of activity that require tailored interventions. While we consider these crimes as distinct, we recognise there are points of intersection in the Government's response to addressing these harms. We are encouraged by the explicit intention to align approaches and reduce regulatory overlap or conflict.

4.2. DIGI has worked extensively on scam prevention and consumer protection. DIGI's members invest heavily in protecting Australian consumers from scams. Approaches are diverse (just like the digital industry itself) but often include: safety-by-design, policies and reporting, consumer education and digital literacy, and proactive detection.

4.2.1. In 2024, DIGI launched the *Australian Online Scams Code* (AOSC), a proactive consumer protection measure, establishing a blueprint for combatting scams in the digital industry.[4]

4.2.2. In the same year, DIGI published a guide with steps to report potential scams to relevant DIGI members in a guide for Australian consumers.[5]

4.2.3. As well as representing our members' efforts, DIGI is also a proud representative of the Advisory Board of the ACCC National Anti-Scams Centre (NASC), as well as several of its working groups.[6]

4.3. DIGI supports close collaboration between industry, civil society, law enforcement, consumers, and government to understand and respond to complex issues such as scams, identity theft, and other cyber incidents. DIGI sits on the NASC Advisory Board alongside IDCare, an organisation providing essential frontline support to Australians for identity theft and cyber related issues.[7] In response to consumer reports, IDCare assesses a situation and develops a tailored response plan to help guide the affected party. Services, such as IDCare, provide affected consumers with support to navigate the financial and emotional uncertainty associated with identity theft. DIGI encourages continued government support of essential frontline support from organisations, such as IDCare.

4.4. The Discussion Paper acknowledges that the Australian Government must work closely with State and Territory Government partners as joint stewards of Australia's government response to cyber security, DIGI also encourages this continued level of collaboration as it relates to identity theft.

4.5. Compromised identity documents play a key role in identity theft crime. These identity documents could encompass both state issued ID; such as licenses or photo cards, or Australian Government issued ID; such as passports. Consideration could be given to coordination between Federal, State and Territory governments and local law enforcement when an ID document is reported stolen or compromised.

4.6. DIGI applauds the Government introducing the Credential Protection Register that helps protect people whose personal details and credentials have been stolen by 'locking down' the stolen credentials. We note the register has blocked over 300,000 attempts to use stolen credentials for fraudulent purposes.[8]We also note the NSW State Government has also introduced a register under the *Identity Protection and Recovery Bill 2025.*[9] Consistent expansion of similar protections across all Australian States and Territories could provide consumers with stronger support and protections.

4.7. In considering regulatory cohesion, DIGI also encourages the Government to carefully consider the continued development and design of the *Scam Prevention Framework.* For example, DIGI has stressed that careful consideration needs to be given to how any scam

[4] https://digi.org.au/scams/
[5] Ibid.
[6] https://www.nasc.gov.au/what-we-do/how-were-run
[7] https://www.idcare.org/
[8] https://www.dataanddigital.gov.au/plan/progress/protecting-australians
[9] https://legislation.nsw.gov.au/view/html/bill/9c15f968-3f87-4e7e-9a0f-974338f5bd35

prevention related obligations are designed.

4.8. We are committed to working constructively with the Government on a robust, effective and proportionate framework. Industry remains in close consultation with the Treasury on the progression of the *Scam Prevention Framework*, including the appropriate ecosystem design for data collection and intelligence sharing so as to prevent cyber risks through cross-sectoral data sharing. We encourage the Department to closely coordinate with the Treasury on the relevant intersections of the framework with cybersecurity strategy.

Australia's domestic and international opportunities

5. Interoperability and best practice governance

5.1. DIGI welcomes the Government's recognition of the value and importance of international cybersecurity regulatory alignment. International interoperability, partnership and engagement are essential to Australia's role in the global cybersecurity ecosystem and ensuring best practices in governance. DIGI has previously emphasised and maintains our position on the importance of interoperability in Australia's approach to cyber security, especially the globalised nature of the manufacture and distribution of relevant products and services.

5.2. DIGI has long supported globally interoperable standards for IoT, edge devices, and consumer energy resources, building on the ETSI EN 303 645 baseline. Interoperability minimises compliance costs and supports secure-by-design principles. DIGI has long supported the first three principles of the ETSI EN 303 645 standard, which are now mandated baseline security standards in Australia, namely to:

5.2.1. Ensure that smart devices do not have universal default passwords;

5.2.2. implement a means to receive reports of cyber vulnerabilities in smart devices; and

5.2.3. provide information on minimum security update periods for software in smart devices.

5.3. Previously in this submission (2.5.2), DIGI has cited the ITI paper, *Cyber Security Labelling: A Guide for Policymakers.* This paper highlights the necessity of interoperability of cybersecurity regimes with allies and like-minded governments. ITI cautions that, if not consulted upon properly, labelling schemes can cause barriers to trade in a global marketplace. In this context, it is worth remembering that Australia is a major importer of technology.[10]

5.4. Aligning Australia with international standards, results in stronger cyber security outcomes for consumers without presenting significant risks to global trade or unnecessary burden on manufacturers.

5.5. We recognise that labelling is not specifically in the scope of this discussion paper, however we suggest these considerations are generally relevant to the development of

[10] https://www.dfat.gov.au/sites/default/files/australias-goods-services-by-top-25-imports-2023-24.pdf

cybersecurity schemes given the relevance of global manufacturing and supply chains to the production of internet connected devices.

5.6. As previously noted, we must strive for interoperability with our cyber security consumer protections, otherwise we risk creating barriers to trade. We need to pull levers that maximise the business opportunities in creating and expanding technology companies in Australia, minimise their risk, and optimise global interoperability of regulatory settings.

6. Australia should continue to prioritise international forums

6.1. DIGI encourages continued Australian leadership in international forums and multilateral partnerships, such as the OECD and the Quad, leveraging existing collaboration channels to promote interoperable cyber norms and remain engaged in the development of international standards, such as those produced by the ISO.

6.2. DIGI also considers that the Government should consider joint disruption operations targeting transnational cybercrime, such as offshore fraud operations. A whole-of-Government approach, that works with industry, should target international crime networks to stop cybercrime at its source.

1.1. We believe there is benefit in identifying Australian expert stakeholders to represent domestic interests in these processes and welcomed the Government's intention to bolster the engagement of Australian experts in relevant international forums. This will ensure that Australia remains in step with international standards and is best placed to participate in the global ecosystem.

Conclusion

6.3. DIGI appreciates the opportunity to contribute to the development of Horizon 2 of the *2023–2030 Cyber Security Strategy*. To summarise our recommendations in this submission:

6.4. **Cyber security capability and education**

6.4.1. Scale consumer and small business awareness and education initiatives.

6.4.2. Continue consistent, evidence based cyber security messaging for consumers, businesses, and industry.

6.4.2.1. We recommend these emphasise practical behaviours (e.g. two-factor authentication, strong passwords, updates).

6.4.3. Maintain a partnership-based approach, consulting closely with industry.

6.5. **Regulatory clarity and coherence**

6.5.1. Continue engagement with relevant Departments, such as Attorney-General's Department and the Treasury on the overlap present between privacy, scams and cybersecurity regulations to reduce overlap and complexity.

6.5.2. Distinguish unauthorised fraud (hacking/data breaches) from authorised scams to ensure clarity in policy responses to each issue.

6.6. **International alignment and global engagement**

6.6.1. Maintain active participation in international forums (OECD, Quad, ISO) to shape norms and standards.

6.6.2. Support joint disruption of transnational cybercrime networks.

6.6.3. Pursue globally interoperable standards to reduce compliance costs and strengthen outcomes.

6.7. Our members remain committed to collaborating with the Government to deliver a cyber security ecosystem that supports innovation, protects consumers, and enhances Australia's position as a global cyber leader. We welcome continued dialogue on the implementation of Horizon 2 initiatives and stand ready to provide technical expertise and industry insights as the consultation process progresses and policies and programs are developed.