To: Australian Cyber Strategy Team
Department of Home Affairs
By email: auscyberstrategy@homeaffairs.gov.au

Wednesday April 19, 2023

Dear Australian Cyber Strategy Team,

The Digital Industry Group Inc. (DIGI) thanks you for the extended opportunity to provide our views on the *2023– 2030 Australian 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, eBay, Google, Linktree, Meta, TikTok, Twitter, Spotify, Snap 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 has engaged in previous consultations in relation to Australia's cyber security strategy, including the 2021 Department of Home Affairs' discussion paper *Strengthening Australia's cyber security regulations and incentives*, and the 2022 National Data Security Action Plan Discussion Paper. Our input to those processes is relevant to many of the 2023's Discussion Paper's questions and we trust that it will be considered, along with other stakeholder input.

In relation to previous consultations, DIGI was concerned to see the inclusion of data localisation in the Data Security Discussion Paper; we welcome that it has not been explicitly explored in this Discussion Paper. DIGI is of the firm view that the physical location of data does not make it inherently more or less secure; what matters most are technological controls and policies to ensure security and privacy. Conversely, data localisation can make data more susceptible to attack, as a further centralisation within known data centres can make them a target for cyber attacks.

DIGI recognises the contextual changes that occurred in late 2022 that have shifted the focus of the strategy in the most recent Discussion Paper. Recent large-scale data breaches in the telecommunications and insurance sectors have underscored the critical importance of data privacy and cyber security economy-wide, and the serious impact that any such event can have on Austalians. DIGI considers that a key area of focus in this strategy should be improved cyber security incident response and communication channels between industry and Government.

These data breach events have underscored the importance of data minimisation, as the more information that is required to be collected and retained by companies can increase the severity of a potential breach. 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).

DIGI also sees an exciting opportunity for increased mandatory cyber security and related obligations in the current reform of the Privacy Act, in order to level up controls and processes within all entities subject to that Act. In our submission on the Privacy Act Reform Report, which we would be happy to make available to the Australian Cyber Strategy Team, we welcomed all of the proposals aimed at improving the security, retention and destruction of personal information, as outlined in Section 21 of the Report. We also welcomed the reinforcement of the data minimisation principle in the Report, which we consider of critical importance to reducing the human impact of data breaches. We see the Privacy Act reform process, particularly with its expanded application through the removal of many of the current exemptions to the Privacy Act, as a critically important opportunity to improve cyber security protections for Australians economy-wide. It is therefore of central relevance to the 2023– 2030 Australian Cyber Security Strategy.

With the recent experience of data breaches in front of mind, DIGI understands that one of the key questions being contemplated in the 2023 Discussion Paper is whether there is an effective framework through which the Federal Government and industry can work together when there is a cyber incident in order to enable a national response. DIGI supports the need for regulation to assist a national response to cybersecurity incident; however, we consider that the framework for the regulation already exists under the Security of Critical Infrastructure Act 2018 (SOCI), the reformed Privacy Act (with the adoption the proposals in Section 21 of the report and removal of exemptions), and the existing Notifiable Data Breaches scheme. We are concerned that the addition of a Cyber Security Act will add complexity to these three regulatory frameworks, and would not further the goal of improving clarity following a cyber incident.

The Department might consider a thorough gap analysis to inform the best approach to improve incident response. For example, the Discussion Paper seeks views on whether further developments to the SOCI Act are warranted, such as including customer data and 'systems' in the definition of critical assets; however, DIGI is of the understanding that these assets are already covered under SOCI through the definition of 'asset' which includes "a system, network, facility, computer, computer device, computer program, computer data, premises and "any other thing"[1].

As noted, DIGI considers that a key area of focus of the strategy should be around improving the communication channels between industry and Government after cyber security incidents. In light of the different regulatory frameworks described above that cover different entities across the economy, we encourage the Government to adopt a 'no wrong door' approach that provides a central, well-publicised, and well-resourced portal through which industry can report incidents, and where the involvement of relevant Government stakeholders is centrally managed by a lead agency. DIGI welcomed the announcement of a coordinator for Cyber Security, supported by a National Office for Cyber Security within the Department of Home Affairs, and we see this as a logical office to lead its coordination, and we encourage its resourcing accordingly.

[1] Department of Home Affairs, *CISC Factsheet - The Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*, available at https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-factsheet-security-legislation-amendment-critical-infrastructure-protection-act-2022.pdf

DIGI welcomed the elevation of the cyber security portfolio to have an assigned Minister, and we have previously advocated for the reintroduction of this Ministerial position. To date, it has not always been clear where the responsibilities for Australians' cyber security lie across Government, as today responsibilities related to cyber security fall across the Australian Cyber Security Centre in the Australian Signals Directorate, the Attorney General's Department, the Office of the Australian Information Commissioner, the Australian Competition and Consumer Commission, the Office of the eSafety Commissioner, the Department of Communications and the Department of Home Affairs. Closer coordination across all relevant security, safety and privacy efforts is needed in order to ensure that plans are cohesive, an efficient use of resources, and conducive to evaluation, and that cyber incidents can be effectively managed.

DIGI has focused its response to this submission on several of the discussion questions in relation to incident response, and 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 that should form an important pillar of the overarching strategy.

We thank you for your consideration of the matters raised in this submission. Should you have any questions, please do not hesitate to contact me.

Best regards,

[redacted]

Sunita Bose
Managing Director, DIGI
[redacted]