The Australian Industry Group
Level 2, 441 St Kilda Road
Melbourne VIC 3004
PO Box 7622
Melbourne VIC 3004
Australia
ABN 76 369 958 788

10 June 2022

Data Security and Strategy
Department of Home Affairs
Email: datasecurityandstrategy@homeaffairs.gov.au

Dear Sir/Madam

NATIONAL DATA SECURITY ACTION PLAN DISCUSSION PAPER

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission to the consultation on the Discussion Paper, *National Data Security Action Plan*, by the Department of the Home Affairs (Home Affairs). We also appreciated the opportunity to attend the townhall briefing held by the Department in May.

Our members are businesses of all sizes and many sectors across Australia. Given the growing engagement across the business community with every business having the capability of having a digital business or platform, accelerated by the COVID-19 pandemic, we are particularly focussed on the implications for the broader cross-section of Australian businesses. This is not limited to only large technology companies, but also SMEs and businesses from a range of sectors.

Overall, industry recognises the importance of protecting the privacy, safety and security of the Australian community, both in the physical and online realm. Indeed, Ai Group works closely with governments and their bodies in a diverse range of areas.

We support a data stewardship regime that benefits both customers and businesses, irrespective of the specific regime. The regulatory environment should also be conducive to the promotion of digital investment, innovation and competition that benefits industry and the community in the long term. In principle, we therefore support the intention behind the Discussion Paper to ultimately protect data.

The COVID-19 pandemic has also presented an additional impost on businesses that needs to be taken into consideration. We are mindful of consequences that new forms of regulation could have for businesses that are already stretched in meeting the needs of the Australian community during this pandemic. Additional unnecessary regulatory costs could stifle business investment, innovation and competition, while providing little value (if any) to the community.

For the purposes of this consultation, our submission provides preliminary comments regarding regulatory matters related to data security. As this consultation progresses, we look forward to further development and understanding of material issues and underlying causes (if any), followed by an exploration and assessment of potential options to address these including regulatory impact and cost benefits assessment.

We would also welcome our continued inclusion in further consultations and the opportunity to work closely with the Government, and relevant members covering a wide range of sectors and other stakeholders that may be impacted by data security.

1. Interrelated regulatory activities

The Discussion Paper offers a useful stocktake of the current landscape of regulation associated with data stewardship. It rightly acknowledges the various interrelated reforms, Australian government data bodies, legislations, regulations and frameworks (such as action plans and strategies) that are in place or underway.

We consider that there are similar issues considered in these various reforms (albeit from different perspectives) that would be pertinent to this consultation. Without necessarily reiterating our previous comments, we include in Appendix A to this submission a list of interrelated consultations where we have made submissions (2019 to 2022).

For example, the Discussion Paper raises several topics with supporting questions that are covered in other consultations, including: protections (not limited to data, cyber and security); scope (including definition of data and extent of proposed obligations); existing best practices (including standards); and international obligations and approaches (including data protection and security frameworks, standards, digital trade and cross border data flows). We consider that these topics have been raised in consultations such as: Attorney-General Department's Privacy Act Review and online privacy reforms; Department of infrastructure, Transport, Regional Development and Communications' online safety reforms; Home Affairs' *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act) reforms; Home Affairs' cyber incentives and regulations consultation; Treasury's Consumer Data Right reforms; and AI related consultations.

Further, while the Discussion Paper offers a stocktake of Federal regulations associated with data stewardship, we would encourage the Department to also include considerations of how State legislative frameworks and industry-specific standards interact with Federal regulatory activities.

2. Coordinating regulatory body and industry assistance

As noted above, the Discussion Paper recognises various Australian government bodies that have an interest in data security. In this regard, we consider that it would be productive if there were improved coordination between the relevant government bodies to provide more regulatory certainty to industry, reduce regulatory red tape and ensure proper balance be given to boost industry especially as it recovers from the pandemic. If implemented effectively, a more coordinated approach would address the questions raised in the Discussion Paper regarding legislative and policy measures, harmonisation of approaches, clear accountability between government bodies, and industry assistance.

We most recently highlighted the importance of a more coordinated approach towards a range of digital and cyber related reforms including in the SOCI Act reforms.[1]

In particular, we noted that proper stakeholder consultation on these interrelated reforms could include assessing the merits of establishing a central regulatory body under a central government department such as the Department of Prime Minister & Cabinet (PM&C) that can properly coordinate between the various regulators responsible for developing codes and regulations. This could provide a more holistic approach including understanding the cumulative regulatory impacts and costs on affected stakeholders who may be subject to multiple regulations related to online activities, which can act as a collective barrier to business digital investment and global competitiveness. The PM&C also plays an important role, providing oversight of the Digital Economy Strategy, Australian Data Strategy and Critical Technologies Blueprint and Action Plan, so this coordinating approach could be another advantage.

Alternatively, as at 1 June 2022, we note that the Department of Industry, Science and Resources is now responsible for national policy issues relating to the digital economy, and the Department of Finance now manages whole-of-government deregulation policy coordination; while Home Affairs maintains responsibility for cyber policy coordination and critical infrastructure protection coordination, and the Department of Foreign Affairs and Trade maintains management of international security issues including cyber affairs. This presents an important opportunity to review how these areas can be properly coordinated, especially in the context of a coordinating regulatory body.

The impact of introducing regulatory reforms need to also be properly considered against other government initiatives that are designed to help boost industry capability, investment and competitiveness. If regulatory reforms result in a negative impact on the objectives and benefits of these other initiatives, these will need to be publicly accounted for. This includes broader initiatives such as the Government's deregulation/red tape reduction policy, COVID-19 economic recovery and

[1] Ai Group submission to PJCIS on SOCI Act reforms (25 February 2022): https://www.aigroup.com.au/news/submissions/2022/submission-to-pjcis-on-critical-infrastructure-protection-bill/.

sovereign industrial capability agendas, as well as meeting the visionary challenge set by the previous Australian Government for Australia to become a digital economy leader by 2030.

As an example, a positive practical outcome from a more coordinated approach could be simplification and streamlining of the reporting avenues to governments and/or other relevant bodies when incidents occur related to data security i.e. via Notifiable Data Breaches, SOCI cyber reporting, ransomware reporting, and other regulatory requirements.

Other measures may also include transitional assistance for companies to meet new forms of regulatory compliance that may impact on an expanded range of businesses. For example, businesses may need to increase or upskill personnel capability to help them properly meet new regulatory obligations. This will be especially important for companies that are not traditionally subject to these types of reforms, which will need as much assistance as possible. It is important to note that this is not necessarily about just providing funding to deliver practical uplift support to large technology businesses, but also about SMEs and wider industry that may be impacted.

3. Additional comments

In addition to the above, the following are specific points that may benefit through further consideration:

- Government handling of data – In circumstances where entities are compelled to provide commercially sensitive data to government for regulatory compliance purposes, there will be concerns about the type of requested information and how it will be adequately protected. This particular issue was raised during the SOCI Act reforms.[2]

- Consistency in terminology –The Discussion Paper raises a principles-based framework built on three pillars i.e. accountability, security and control. Was this framework established through reference to existing standards or frameworks such as NIST and ISO 27001 or are these new concepts? Often the same words can have different definitions under different government bodies. It would be beneficial for businesses if common data security terminology were utilised across the whole of government.

- Cohesion in procurement requirements – Another example where there could be effective harmonisation between different Australian jurisdictions with respect to cyber security (including data security) is in government procurement requirements. In a previous submission to Home Affairs, we shared an anecdote of specific problems for businesses having to comply with multiple cyber security standards if they are (or want to be) involved in various government procurement projects. This problem appears to be prevalent across various government levels and jurisdictions. For businesses (from SMEs to large) wishing to tender for various government projects, meeting multiple cyber security standards can become a very costly exercise and inadvertently an even greater barrier for SMEs in being given full and fair access to government procurement. Therefore, it would be greatly beneficial if the various cyber security standards requirements across the various government agencies and jurisdictions could be harmonised.

- Data breaches – Data breaches falls under the scope of the Notifiable Data Breaches Scheme under the *Privacy Act 1988* (Cth) and a subject for discussion as part of the AGD's Privacy Act Review. Nevertheless, it is worth noting that we have made several recommendations to the AGD as part of their review, as well as previously with Home Affairs, regarding how Government can provide assistance including in terms of cyber security.[3]

---

[2] See Ai Group submission: https://www.aigroup.com.au/globalassets/news/submissions/2022/supplementary_sub_pjcis_critical_infrastructure_protection_bill_march2022.pdf.

[3] See Ai Group submissions: https://www.aigroup.com.au/globalassets/news/submissions/2021/strengthening_australias_cyber_security_27aug_2021.pdf and https://www.aigroup.com.au/globalassets/news/submissions/2022/privacy_act_review_discussion_jan2022.pdf.

- Data centres – We note that the data storage and processing sector has been added as a sector along with assets that are covered under the SOCI Act reforms. This may cover data centres subject to certain criteria in terms of critical infrastructure security.

- Data localisation – In addition to consideration of security associated with data centres, caution needs to be given regarding data localisation policy. For example, entities with a global presence and therefore globally connected may have difficulties in segregating Australian based data and overseas data. This could occur if they have a parent organisation overseas, as well as if they share common networks. This could also have broader implications with respect to cross border data flows, digital trade, as well as enabling sharing of data between Australia's international partners.

- Digital trade regulatory activities – Ai Group has been working with like-minded associations around the world to advocate for the permanent moratorium on applying customs duties on electronic transmissions. We refer Home Affairs to the OECD's Trade Policy Brief regarding this matter.[4] Ai Group is also working on more general global coherence in digital regulation. The OECD and WTO are jointly undertaking an analysis of the impact of cross-border data regulation on economic activity and seeking business feedback.[5] The aim of the consultation is to help policy-makers better understand the emerging challenges that businesses face, which will be used to shape and design policies that can enable data to flow across borders with "trust".

- Supply chains – Supply chain security has been discussed in different forums. This includes Home Affairs' cyber security incentives and regulations consultation. Most recently, the matter has been discussed as part of the SOCI Act reforms.

- Skills shortage – Many reports highlight the challenges to having sufficient skills and talent in Australia, which has been negatively exacerbated by the impact of COVID-19 and regulatory responses. This has been further compounded with Australia competing for talent locally and overseas across businesses, sectors and governments. Introduction of new regulation presents further challenges to entities as they seek the necessary talent and skills to immediately meet regulatory requirements. Government needs to be cognisant of this skills shortage issue, which is not limited to the subject of data security.

If you would like clarification about this submission, please do not hesitate to contact me or Charles Hoang (Lead Adviser – Industry Development and Defence Industry Policy, charles.hoang@aigroup.com.au).

Yours sincerely,

Louise McGrath
Head of Industry Development and Policy

[4] See OECD, "The Case for the E-Commerce Moratorium" (Trade Policy Brief, May 2022), https://issuu.com/oecd.publishing/docs/moratorium_policy_brief.
[5] OECD and WTO Business Consultation on Cross-Border Data Flows and Trade, https://survey.oecd.org/index.php?r=survey/index&sid=294791&lang=en.

Appendix A: List of Ai Group submissions (2019-2022) on interrelated reforms

- AI:
  - Department of the Prime Minister & Cabinet (PM&C) Issues Paper on Positioning Australia as a leader in digital economy regulation – Automated Decision Making and AI Regulation (2022): https://www.aigroup.com.au/globalassets/news/submissions/2022/pmc_ai-and-adm_regulation_issues_paper_29apr_2022.pdf
  - Department of Industry, Science, Energy and Resources (DISER) Discussion Paper on AI Action Plan (2020): https://www.aigroup.com.au/globalassets/news/submissions/2020/diser_ai_action_plan_dec2020.pdf
  - AHRC (Australian Human Rights Commission) Discussion Paper on Human Rights and Technology (2020): https://www.aigroup.com.au/globalassets/news/submissions/2020/ahrc_human_rights_and_technology_discussion_paper_26mar_2020.pdf
  - Standards Australia Discussion Paper on Developing Standards for AI (2019): https://www.aigroup.com.au/globalassets/news/submissions/2019/aigroup_submission_standards_australia_ai_standards.pdf
  - DISER Discussion Paper on the Australian AI Ethics Framework (2019): https://www.aigroup.com.au/globalassets/news/submissions/2019/ai_group_submission_ai_ethics_framework_discussion_paper.pdf
  - AHRC and World Economic Forum White Paper on AI Governance and Leadership (2019): https://www.aigroup.com.au/globalassets/news/submissions/2019/aigroup_submission_ahrc_whitepaper_ai_governance_and_leadership.pdf

- Consumer Data Right (CDR):
  - Treasury Consultation Paper on Strategic Assessment on Implementation of an Economy-wide CDR (2021): https://www.aigroup.com.au/globalassets/news/submissions/2021/cdr_strategic_assessment_consultation_paper_1sep_2021.pdf
  - Treasury Issues Paper on Inquiry into the Future Directions for the CDR (2020): https://www.aigroup.com.au/globalassets/news/submissions/2020/treasury_cdr_inquiry_5jun_2020.pdf

- Critical infrastructure security:
  - Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill (SLACIP Bill) (2022): https://www.aigroup.com.au/globalassets/news/submissions/2022/pjcis_critical_infrastructure_bill_25feb_2022.pdf; https://www.aigroup.com.au/globalassets/news/submissions/2022/supplementary_sub_pjcis_critical_infrastructure_protection_bill_march2022.pdf
  - Home Affairs Exposure Draft of the SLACIP Bill (2022): https://www.aigroup.com.au/globalassets/news/submissions/2022/critical_infrastructure_protection_bill_feb2022.pdf
  - PJCIS Review of the Security Legislation Amendment (Critical Infrastructure) Bill (SLACI Bill) (2021): https://www.aigroup.com.au/globalassets/news/submissions/2021/sub-41---australian-industry-group.pdf; https://www.aigroup.com.au/globalassets/news/submissions/2021/review_security_legislation_amendment_bill_26july.pdf
  - Home Affairs Draft Critical Infrastructure Asset Definition Rules (2021): https://www.aigroup.com.au/globalassets/news/submissions/2021/home_affairs_draft_critical_infrastructure_assets_definition_rules_13may.pdf
  - Home Affairs Exposure Draft of the SLACI Bill (2020): https://www.aigroup.com.au/globalassets/news/submissions/2020/home_affairs_critical_infrastructure_security_reforms_exposure_draft_bill_nov2020.pdf
  - Home Affairs Consultation Paper on Protecting Critical Infrastructure and Systems of National Significance (2020): https://www.aigroup.com.au/globalassets/news/submissions/2020/dept_home_affairs_critical_infrastructure_security_reforms_sept2020.pdf

- Cyber security:
  - Home Affairs Discussion Paper on Strengthening Australia's Cyber Security Regulations and Incentives (2021): https://www.aigroup.com.au/globalassets/news/submissions/2021/strengthening_australias_cyber_security_27aug_2021.pdf
  - Home Affairs Discussion Paper on Critical Technology Supply Chain Principles (2020): https://www.aigroup.com.au/globalassets/news/submissions/2020/home_affairs_critical_technology_supply_chain_principles_discussion_paper_12nov.pdf
  - Home Affairs Discussion Paper on the 2020 Cyber Security Strategy (2019): https://www.aigroup.com.au/globalassets/news/submissions/2019/2020_aust_govt_cyber_security_strategy_discussion_paper_1nov_2019.pdf
  - PJCIS Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act (2019-20): https://www.aigroup.com.au/globalassets/news/submissions/2020/sub-23.1---ai-group-3.pdf; https://www.aigroup.com.au/globalassets/news/submissions/2019/aigroup_submission_inslm_review_tola_act.pdf; https://www.aigroup.com.au/globalassets/news/submissions/2019/pjcis_assistance_access_bill_review_2019.pdf
  - PJCIS Review of the Telecommunications Legislation Amendment (International Production Orders) Bill (2020): https://www.aigroup.com.au/globalassets/news/submissions/2020/sub-32---ai-group-3.pdf
  - Home Affairs Draft Code of Practice on Securing the Internet of Things for Consumers (2020): https://cdn.aigroup.com.au/Submissions/Technology/Securing_IoT_for_Consumers_Voluntary_Code_of_Practice_Feb_2020.pdf

- Digital platforms:
  - ACCC Final Report on the Digital Platforms Inquiry (2019): https://www.aigroup.com.au/globalassets/news/submissions/2019/aigroup_submission_digital_platforms_inquiry.pdf
  - ACCC Preliminary Report on the Digital Platforms Inquiry (2019): https://www.aigroup.com.au/globalassets/news/submissions/2019/gaca-statement-revised-as3996-2019-002-2.pdf

- Online Safety:
  - Department of infrastructure, Transport, Regional Development and Communications (DITRDC) Exposure Draft of the Online Safety (Basic Online Safety Expectations) Determination (2021): https://www.aigroup.com.au/globalassets/news/submissions/2021/draft_online_safety_determination_2021_12nov.pdf
  - Senate Standing Committees on Environment and Communications Inquiry on the Online Safety Bill (2021): https://www.aigroup.com.au/globalassets/news/submissions/2021/senate_standing_committees_on_environment_and_communications_inquiry_on_online_safety_bill.pdf
  - DITRDC Exposure Draft of the Online Safety Bill (2021): https://www.aigroup.com.au/globalassets/news/submissions/2021/draft_online_safety_bill.pdf
  - DITRDC Discussion Paper on the Online Safety Act (2020): https://www.aigroup.com.au/globalassets/news/submissions/2020/new_online_safety_act_proposals_21feb_2020.pdf

- Privacy:
  - Attorney-General's Department (AGD) Discussion Paper on Review of the Privacy Act (2022): https://www.aigroup.com.au/globalassets/news/submissions/2022/privacy_act_review_discussion_jan2022.pdf
  - AGD Exposure Draft of Online Privacy Bill (2021): https://www.aigroup.com.au/globalassets/news/submissions/2021/online_privacy_bill_6dec_2021.pdf
  - AGD Issues Paper on Review of the Privacy Act (2020): https://www.aigroup.com.au/globalassets/news/submissions/2020/privacy_act_review_november_2020.pdf