Australian Computer Society Inc. (ACT)
ARBN 160 325 931

National Secretariat
Tower One, 100 Barangaroo Avenue, Sydney NSW 2000
PO Box Q534, Queen Victoria Building, Sydney NSW 1230
T +61 2 9299 3666 | F +61 2 9299 3997
E info@acs.org.au | W www.acs.org.au

To the Australian Department of Home Affairs

ACS Response
National Security Action Plan Discussion Paper

10 June 2022

Dear Sir or Madam

Thank you for the opportunity to contribute to this critical discussion.

The Australian Computer Society (ACS) is the peak professional association for Australia's information and communications technology sector, with over 43,000 members working in all technology fields.

We're very pleased to see the Department taking this critical issue seriously – national security is a whole-economy issue, not just a matter for government departments. Guidance and assistance, along with hard rules, are critical elements to ensuring that Australians business can meet compliance obligations while Australian citizens can feel that their personal data and identity is safe.

In the following pages, we have presented some recommendations and considerations for the Department on this matter. These recommendations are the work of our expert members, and we hope that they can be helpful as the Department continues its important oversight and planning duties.

Thank you for your time and the opportunity to comment on the proposals. If you would like to discuss any part of this response or simply seek further clarification or input, please feel free to contact myself by email at troy.steer@acs.org.au or by phone on 0417 173 740.

Yours sincerely

Troy Steer
Director of Corporate Affairs and Public Policy
Australian Computer Society

Responses to key questions

Please see below for responses to some of the key questions posed in the National Security Action Plan Discussion Paper. Please note that not all questions have been answered.

1.	**What do you consider are some of the international barriers to data security uplift?**	There are a number of barriers that will need to be overcome, including: 1.1 Inconsistency due to the complexity and diversity of legislation around the world. This is a barrier to security uplift; therefore reducing complexity should be a principal objective of any international efforts. This might include: 1.1.1 Advancing a minimum requirement, based on industry accepted standards such as mandated encryption standards. 1.1.2 Establishing and communicating a baseline of internationally-recognised standards. 1.1.3 Developing resources and guidance for implementing mandated standards. 1.1.4 Consideration of establishing principles that can be applied to make the implementation more consistent and easier. 1.1.5 Building on what standards already exist, and avoiding the creation of Australia-specific standards. 1.1.6 Prioritisation of mandated international standards to be applied and implemented. 1.1.7 Having a program and incentives already in place for maintaining and keeping the security practices up to date. 1.2 Jurisdictional issues. Can the ability to prosecute people or organisations in other countries be enabled? 1.3 Multiple legislated obligations. Australia should: 1.3.1 Consider internationally harmonised legislation; eg. GDPR (Europe), GDPR (UK), GDPR (Australia). 1.3.2 Examine how Europe and UK GDPR legislation has been enabled and its effectiveness, strengths and weaknesses.
2.	**How can Australian Government guidance**	Per 1.3 above, we recommend the Australian Government actively pursue having internationally consistent legislation as a means of

	best align with international data protection and security frameworks? Are there any existing frameworks that you think would be applicable to Australia's practices (e.g. the European Union's General Data Protection Regulation)?	applying controls and practices that would support trade and the economy and enable business to benefit from a lower cost of compliance. The government could consider a two-tiered approach, having a higher-level framework in place. For example, NIST could be used as a foundation, with industry specific standards specifically applied.
3.	**What additional guidance or support from Government would assist you to meet a principles-informed approach to data security? How would this be delivered best to you?**	Not answered.
4.	**How could Australian legislative and policy measures relating to data security be streamlined to better align with your obligations in international jurisdictions? Does variation in international approaches create hurdles to your effective participation in the global market? a. What obligations are you most commonly subjected to from international jurisdictions?**	Europe's GDPR has been mirrored in UK legislation. Consideration for enhanced streamlining of obligations in international jurisdictions would or could be addressed with Australian legislation based on the GDPR (Europe/UK). This would assist in international trade agreements and business.
5.	**Does Australia need an explicit approach to data localisation?**	Yes. Data localisation that respects data sovereignty and enables the privacy of citizens and confidentiality of their records needs to be maintained. This localisation regime would need to consider the sensitivity of the data and the ability for multinational organisations to protect the data, while not imposing excessive costs and duplication for separate jurisdictional data holdings. There are also special cases in Australia concerning cultural sensitivities that must be considered. For example, some Koorie information should not be circulated beyond specific zones. Cultural sensitivities should be built into data and security requirements.

6.	**How can data security policy be better harmonised across all jurisdictions? What are the key differences between jurisdictions that would impact the ability to implement standardised policies/are there any areas of policy that could not be standardised?**	Leadership across the States, Territories and Commonwealth Government is necessary to achieve a preferred future for cyber and data security practices. Consistency in the policy and its application, underpinned by legislation and regulations, will be preferred and necessary to encourage efficiencies and common practices. Ideally, these would be based on IEC/ISO and other internationally recognised cyber and security standards. This will avoid tailored responses by jurisdiction and associated inefficiencies and higher costs of implementation, maintenance and compliance for both industry, government and SMEs.
7.	**Who is currently responsible for ensuring consistent and commensurate uplift of local government data security and how can this be strengthened? Do you think responsibilities should be shared across more bodies, or shifted elsewhere entirely?**	The ability for the community to have a voice is important in this. The social license and obligation for keeping the public's data safe, while fulfilling an obligation for the data to be used for public good, would benefit from greater accountability and transparency. The desired uplift is unlikely to simply be achieved by local government alone, even with the support of trusted non-government service and infrastructure providers. Therefore, a shared responsibility for maintaining appropriate end-to-end cyber and data security in place is required.
8.	**What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of Government, including municipal governments?**	Confusion over compliance requirements is an ongoing issue. In the absence of a single set of recommendations, different levels of government apply different sets of rules, with the unintended result of distrust and uncertainty about data security. For example, the WA and SA jurisdictions do not have privacy legislation, and inconsistencies in the scope of the various jurisdictional privacy legislations present an opportunity for the Australian government to introduce privacy-protecting legislation, penalties and obligations that can be more consistently applied nationally.
9.	**What steps could your business take to better understand the value of the data they process**	Businesses are often unclear on the value of the data they hold. For many, often the only way to value data is to lose it, at which point a court will tell them how much it is worth.

and store? Do businesses have sufficient awareness of their data security obligations?	A recognised and consistent system of data valuation would be a useful guide for business to better understand their risk and liability, and in turn motivate them to perform better on matters of security.
10. How can the Australian Government further support your business to understand the value of data and uplift your data security posture?	Government standards can explain how valuable information is or should be treated. Until enforceable legislative penalties apply, however, it will be a challenge to obtain compliance. ACS is able to assist in the development of sensible, achievable rules, aligned to NIST, CMMI or the ISOs.
11. Does your business appropriately consider data security risks in their supply chains? Is there sufficient public information provided by Government to help your business identify these risks?	The ACS as the peak body for technology professionals in Australia, and we recognise that the interruption to supply chains has direct consequences and serious implications on continued business operations and the ability to maintain digitally enabled services. Therefore it is essential that data security and cyber risks are firstly understood via education programs, and proactively managed with regular assessment and mitigation measures put in place. As a result, cyber and data security risk assessments and mitigation would be necessary to enable the supply chain to be assured, and would benefit from a wholistic and integrated assessment that would include people, process, technology and other dependencies, as seen being impacted from the global lack of CPU chips, and the experience from COVID-19 impacting supply chains, along with the recent energy supply constraints that have wider implications across the economy and the community.
12. Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold).	The challenge for smaller businesses is obtaining the expertise and capability to harden their business operations and ensure appropriate data security practices are implemented and more importantly maintained. A size threshold would be appropriate. The one-size-fits-all approach will not work for Small to Medium Enterprises (SMEs) or sole traders. Therefore a threshold set by number of employees or annual turnover/revenue would be useful. It would enable properly targeted material and provide greater understanding and support (including education, tools and direct assistance) for these smaller businesses and activities. A further assessment or categorisation of the criticality of certain enterprise may also be useful to better target critical resources and industries.
13. Are there any limiting factors that would prevent Australian	As implied in the answer provided in 12., there is a concern that smaller SMEs, individuals (sole traders) and less resourced activities will not be able to employ or contract the cyber and data security

	industry and businesses from effectively implementing an enhanced data security regime?	skilled expertise necessary to either establish or maintain the desired enhanced data security regime. Therefore, a transparent assessment of the most critical and lesser important business and industries would enable targeted education, tools and resourcing to achieve a desired level of capability that could be verified independently and assured.
14.	**Does the Australian Government currently have sufficient public information for consumers and citizens on data security best practice? How can we make that information more easily accessible, usable and understandable?**	The Australian Cyber Security Centre (ACSC) has a remit to provide individuals, families and businesses with advice and direction on cyber secure practices. There would benefit from funding the collection of additional data that better can inform the ACSC's activities, enhancing its effectiveness and utilisation as well as programs to enhance community awareness of the ACSC. We would also recommend the Australian Government assess and possibly extend the pilot cyber curriculum that has been developed in South Australia. Early awareness of and expertise in cyber-issues will better equip Australian businesses in the future. This could be implemented through the Australian Curriculum Assessment and Reporting Authority (ACARA) and the existing Digital Tech Educators program being run through the Australian Computer Society (ACS).
15.	**Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?**	The Office of the National Data Commissioner provides a useful capacity for engaging and improving accountability, informing and educating the wider community and business on trusted data practices. The existing cyber attack and breach notification process through the Australian Cyber Security Centre provides the mechanism for improved community wide understanding of the importance and responsibility for cyber and data security. The recent the Australian government legislative reforms including the Data Availability and Transparency Act 2022 (Cth) also needs to be promoted and implemented, and then its effectiveness independently evaluated. Improving public trust is recognised as a significant ongoing challenge. Certification and greater recognition of Cyber Security Professionals and continued certification and professional development, would contribute to achieving both question 14 and 15's objectives. Accountability is also a key factor. To achieve this, there could be incentives and rewards for industry, government, SMEs, families and individuals, to encourage and promote cyber security acumen, qualifications and efforts.