18 October 2022

Productivity Commission
4 National Circuit
Barton ACT 2600
Australia

CPA Australia Ltd
ABN 64 008 392 452

Level 20, 28 Freshwater Place
Southbank VIC 3006
Australia

GPO Box 2820
Melbourne VIC 3001
Australia

Phone 1300 737 373
Outside Aust +613 9606 9677
Website cpaaustralia.com.au

By email: productivity.inquiry@pc.gov.au

Dear Sir/Madam,

Submission on the Productivity Commission's 5-year Productivity Inquiry: Australia's data and digital dividend

CPA Australia represents the diverse interests of more than 170,000 members working in 100 countries and regions around the world. We make this submission on behalf of our members and in the broader public interest.

While the Productivity Commission's Interim Report (Report) provides valuable recommendations on how to establish Australia as a leading digital economy, several of its recommendations fall short of addressing what we see as core problems. Better digital infrastructure, data management, data skills and digital economy regulation are crucial enablers to digital transformation.

We recommend the Commission include the following actions in its final report:

- strengthen the collaboration between government and industry to attract foreign technology workers while also investing in improving the skills of the Australian workforce.
- shift from an occupation perspective to a skills perspective for migration purposes.
- recognise microcredentials provided by qualified providers as accredited qualifications to demonstrate skills levels.
- introduce small business-specific measures to help them build and improve data literacy and skills to enable them to better use data in their business.
- define the overall objective of implementing security software with in-built automatic cyber incident reporting and assessing how governments and societies benefit.
- reassess whether and how automatic cyber incident reporting adopted by government entities mitigates and manages cyber threats across the economy.
- reform of data security regulations and penalties that is targeted at higher risk organisations managing personal and sensitive consumer data.
- Artificial intelligence (AI) regulation and/or guidance that is aligned with legislation and policies which regulate or impact the use of data and which take account of international developments.
- where regulation of AI is deemed necessary, any associated compliance costs be kept at a minimum.
- make AI and automated decision making (ADM) subject to ongoing governance, reporting and assurance requirements to ensure they remain lawful and up-to-date, and operate as intended.

- harmonise regulation addressing digital, data and cyber security areas across different levels of government.
- improve coordination between government entities and regulators and linking-up of digital economy policy development and consultation.

Our responses to the Interim Report questions are included in the Attachment.

If you have any questions about this submission, please do not hesitate to contact Dr Jana Schmitz, Digital Economy Policy Lead

Yours faithfully

Dr Gary Pflugrath FCPA
Executive General Manager, Policy and Advocacy
Encl.

Attachment

Data Skills

What role (if any) does government have in increasing the number of students and workers undertaking formal and unaccredited education and training in digital and data skills, given that various options are already being offered and taken up?

Government has an important role to play in increasing the digital and data skills of the Australian workforce. Governments, in collaboration with industry and the education sector, must improve our education and training system. It should have a stronger focus on digital and data skills to better prepare today's students and workers for tomorrow's economy and society.

We suggest the government considers the following proposed solutions:

- delivering the Digital Apprenticeship Program to better meet the future needs of jobs in the technology sector
- creating a better definition of skills standards and pathways into careers in the technology sector
- improving support for women to take up or transition into technology jobs, such as the UK's 'Returners Fund'
- conducting ongoing research into and analysis of technology workforce trends.

Regarding skilled migration, government must ensure that it better targets the areas of highest need and greatest demand. We recommend the priority solutions are:

- providing technology workers with accelerated pathways to permanent residency by, e.g. extending the Global Talent visa
- addressing barriers to work for international students studying technology-related courses in Australia
- streamlining skilled migration for experienced technical roles with high salaries.

Recommendation 1

Strengthen the collaboration between government and industry to attract foreign technology workers while building the digital and data skills of the Australian workforce.

How could the skilled migration program be made more relevant to current and future digital and data skill needs — for example, by improving the occupation list or changing how skilled visas are granted?

The Australian Bureau of Statistics (ABS) recently consulted on Emerging Occupations identified by the National Skills Commission (NSC) that were unable to be included in the ANZSCO 2021. The proposed 'emerging occupations' include:

- data analyst
- data scientist
- statistician
- supply chain and logistics analyst
- data architect
- data engineer
- software engineer.

Whilst we don't consider those occupations as 'emerging'—as they are well established—we acknowledge that there is a shortage of such occupations. Attracting workers in listed occupations will contribute to Australia's long-term economic development, the diffusion of innovation and best practice, and global competitiveness. We also note that those 'occupations' are not sector-specific and are therefore likely to lift capabilities across all industries.

Further, in our submission to the ABS on this review, we raise concerns about the ANZSCO skill levels. It is commonly understood that jobs change as global engagement shifts, consumer preferences evolve, technology advances,

employers adopt new and innovative ways of doing business, regulatory requirements change, public expectations alter, and as employees adjust their work habits. Thus, to avoid skills lists becoming increasingly outdated over shorter time periods, the ANZSCO must appropriately accommodate changes to the tasks listed. This is of particular concern given that skilled migration occupation lists are a subset of ANZSCO occupations, and the assessment of prospective migrants are against the skill levels and tasks associated with listed occupations.

Moreover, in our previous submissions[1] on migration matters, we recommend a move away from occupations, given the difficulty of maintaining the currency of those lists, and a move to a focus on skills evidenced by credentials and experience. After all, it's called *skilled* migration and not *occupation* migration.

We expressed our concerns about micro-credentials not being reflected in ANZSCO. As education and training accessed outside of the regulated education system continues to grow (especially in the digital space), micro-credentials become increasingly common both here and overseas. The need to recognise micro-credentials offered by traditional and non-traditional education providers increases significantly in a labor market in which the lifelong learning model will become fully ingrained. In the future, micro-credentials could stack and provide an alternative to accredited qualifications to evidence that the full suite of capabilities or competencies, necessary to enter certain professions and/or Australia as a skilled migrant, have been met.

Recommendation 2:

Shift from an occupation perspective to a skills perspective for migration purposes.

Recommendation 3:

Recognise microcredentials as accredited qualifications to demonstrate skills levels.

Are existing government programs to improve digital literacy adequate, or are some cohorts still at risk of being left behind in an increasingly digitised world?

CPA Australia's 13th annual Asia Pacific Small Business Survey shows that in comparison to small businesses in Asia, Australian small businesses are lagging in their adoption and utilisation of technological solutions. The survey results show that this could be impacting growth in the sector. Recognising the urgency to support small businesses in their digital transformation journey, we suggest that the government improves the data literacy of small businesses through:

- **Encouraging younger people to establish or acquire a small business:** Our survey data shows that younger business owners are far more likely to use technology in their business and benefit from it. Such businesses are often "born digital", i.e., have a digital presence.
- **Strengthening small business ecosystems**: Small businesses need to be embedded in networks comprised of their professional adviser/s, other small businesses, technology vendors, innovation hubs and education providers. They need to have access to relevant support (knowledge, guidance, learning and tools).
- **Tailoring training to small businesses' needs**: Increase education and training offers. Build sustainable training offers that match small businesses' needs (content, form, set-up, resource and time-constraints). Reduce the direct costs of training for small businesses.

Recommendation 4:

Introduce small business-specific measures to help them build and improve data literacy and skills to enable them to better use data in their business.

Cyber Security

How could government work with industry to build automatic cyber incident reporting into security software, and what would be the benefits and costs of this approach?

---

[1] See e.g., submission on the Migration Program 2022-23, submission on the Inquiry into Australia's skilled migration program – part 1 of 2, and submission on the Inquiry into Australia's skilled migration program – part 2 of 2.

Government agencies, as large consumers of digital and data-related products, should place greater focus on cyber resilience and cyber incident reporting. While we understand the intention behind the proposal to build automatic cyber incident reporting into security software, we note that several concerns and questions should be addressed beforehand:

- What is the overall objective of an in-built automatic cyber incident reporting?
- What is being reported (e.g., nature of attack, volume of compromised data)?
- Who owns the reported data (e.g., security software provider, reporting entity)?
- What will the data be used for (e.g., data collection for statistical purposes, law enforcement, developing and sharing of cyber threat intelligence)?
- Whom will relevant data be shared with (e.g., national law enforcement agencies, international authorities)?
- How does the government ensure that the data collected is acted upon (e.g., improvement/ enhancement of government entities' cyber security measures)?
- If the government collaborates with industry, based on what criteria will security software providers be selected (e.g., size, scope, local provider)?
- How does government ascertain that small- and medium-sized security software providers will not be overlooked/disadvantaged?
- Once the investigation into a cyber incident is completed, are mechanisms in place to ensure proper disposal/redress of data collected? If so, what are those mechanisms?

Further, we note that even if government entities implement security software with in-built automatic cyber incident reporting, they may face challenges such as:

- an inability to effectively integrate staff and processes
- false positives creating 'alarm fatigue' among security teams
- hiring and/or training staff to monitor and assess the automatic cyber incident reporting tool
- cost of implementing and maintaining the software.

Recommendation 5:

Define the overall objective of implementing security software with in-built automatic cyber incident reporting and assessing how governments and societies benefit.

We note that cyber security issues arise because points of vulnerability emerge over time within the 'ecosystem' in which multiple parties interact. Cybersecurity settings of each entity within this multiparty ecosystem may lead to vulnerabilities arising elsewhere in the ecosystem. As government entities engage frequently and intensely with private sector entities, we don't see how security software with in-built automatic cyber incident reporting used by government entities only can protect the wider ecosystem.

Mitigation and management of cyber security risks requires government entities to understand whether and how other organisations (public or private) address security risks that arise within a multiparty data handling and processing ecosystem. Given the diversity of actors, increased complexity of end-to-end data supply chains and the variety of contexts and scenarios of technology deployment and data use, an 'in-built automatic cyber incident reporting' approach adopted by government entities only is unlikely to provide appropriate incentives for other entities (public and private) to assess and address evolving cyber security risks.

Recommendation 6:

Reassess whether and how automatic cyber incident reporting adopted by government entities mitigates and manages cyber threats across the multiparty ecosystem.

Lastly, in the wake of the recent Optus data breach incident, we emphasise the need for proportionate reforms to data security regulation. Data security requirements currently placed on large telecommunications providers in Australia are not fit for purpose. A breach of this scale and size should result in more stringent regulatory requirements and penalties for higher risk organisations. However, care must be taken to avoid imposing disproportionate regulatory requirements on lower risk businesses.

Other jurisdictions appear to take data security and privacy more seriously. In the European Union (EU), the General Data Protection Regulation (GDPR) provides the Data Protection Authorities (DPAs) with different options in cases of non-compliance with the data protection rules:

- likely infringement – a warning may be issued
- infringement: the possibilities include a reprimand, a temporary or definitive ban on processing and a fine of up to €20 million or 4 per cent of the business's total annual global turnover.

Stricter regulations and significant penalties for non-compliance for higher risk organisations would at least create disincentives for such organisations to collect large volumes of (often irrelevant) data in the first place and then not store the data properly.

The consequences of identity theft due to data breaches such as the one experienced by Optus customers can be numerous. Affected individuals (and businesses) could be forced to spend months "cleaning up" after data/identity theft and may in fact still experience serious financial and credit problems for years after. In cases where the stolen identity is used to commit other crimes impersonating the victim, affected individuals could even face legal issues.

Individuals and small business should be better supported to seek redress for the harm they suffer due to their data being compromised. This could include compensation for the time and money invested in monitoring bank accounts, MyGov accounts, changing password, applying for new documentation (driver's licence, passport, Medicare card etc.).

Recommendation 7:

Reform of data security regulations and penalties that is targeted at higher risk organisations managing personal and sensitive consumer data.

Ethical use of technology

How should government support the ethical adoption of new uses of technology and data, particularly for applications outside of artificial intelligence?

We question why government would treat the ethical adoption of AI differently from the ethical adoption of new uses of technology and data. Where possible, government policies and regulation should be risk-based, outcome-focused, and technology-neutral.

What would be the benefits and costs of any government activity on technology and data ethics?

The regulatory settings must balance encouraging innovation with safeguarding consumers and the broader community. It should not lead to uncertainty and become a barrier to the development and adoption of technologies.

In our submission to the Department of the Prime Minister and Cabinet's (PMC's) issues Paper on *Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation*, we note that a regulatory framework could enhance the development and uptake of AI in two ways:

(1) effective regulation of (high-risk) AI could increase the community's acceptance of such technology and its deployment in government and the private sector.
(2) aligning AI-specific regulation with the laws of other jurisdictions (e.g., the European Union's Artificial Intelligence Act) would better enable Australian AI providers to export their innovations to other markets and avoid the fragmentation of standards. It would potentially also attract business investments and entrepreneurship from overseas to Australia and enhance local competition by making it easier for foreign AI providers to distribute their innovations in Australia, with minimum or no change necessary.

If the government decides to regulate AI in some way, it's critical that it undertakes a comprehensive cost-benefit analysis before deciding if regulation is necessary and before deciding on the design of such regulation. Small innovators would be deterred from entering the market if compliance costs are high.

Recommendation 8:

AI regulation and/or guidance that is aligned with legislation and policies which regulate or impact the use of data, and which take account of international developments.

Recommendation 9:

Where regulation of AI is deemed necessary, any associated compliance costs be kept at a minimum.

Further, we note that the Commonwealth Ombudsman's Automated decision-making better practice guide, the Digital Service Standard and the AI Ethics Principles are all useful and commendable tools. However, while these tools are generally consistent, they appear to be overseen and managed by different entities. Moreover, none of them are mandated. To the best of our knowledge, it is uncertain whether there is any intent to bring these 'tools' into better alignment to facilitate a more consistent approach, and limited public information is available on the extent of their uptake.

If some regulation is required in Australia on ethical issues, how can the government identify high-risk settings where regulation would be most appropriately targeted?

We agree with the Productivity Commission that the European Union is currently the most active in exploring regulation for ethically responsible uses of technology and data, specifically for AI (see proposed Artificial Intelligence Act). The proposed regulation covers the supply and use of AI. The law is intended to apply to AI used or placed on the EU market, irrespective of whether the providers are based within or outside of the EU. Thus, the regulation has a direct effect on Australia-based AI developers/providers looking to service the EU market.

Regarding the identification of high-risks settings, we suggest that the government also considers the Canadian Directive on Automated-Decision-Making (Canadian Directive). The Canadian Directive requires the person responsible for an AI-based ADM system to conduct an Algorithmic Impact Assessment (AIA) prior to the production of such a system to determine suitability for the deployment of ADM.

The AIA is a questionnaire that determines the impact level of an ADM system. Assessment scores are based on many factors, including systems design, algorithm, decision type, impact and data. The AIA is intended to identify risks and assess impacts in a broad range of areas, including:

- the rights of individuals or communities
- the health or well-being of individuals or communities
- the economic interests of individuals, entities, or communities
- the ongoing sustainability of an ecosystem.

The AIA produces an impact assessment level of the ADM system on the affected interest areas – from little to no impact (e.g., impacts which are 'reversible and brief') to very high impact (e.g., impacts which are irreversible and are perpetual). Critically, the impact assessment level attributed to an ADM system will determine the Impact Level Requirements imposed to regulate the system. For example, the greater the impact assessment level the more onerous the requirements relating to:

- obligation to give notice to affected persons and the content of such notices
- human involvement (higher impact systems require human intervention and certain decisions must be made by humans)
- explanation for a decision (made by ADM or a human)
- training
- contingency planning.

This approach is consistent with the OECD Recommendation, which provides that organisations which deploy AI should include a risk management approach to address risks related to AI systems, including privacy, digital security, safety and bias. CPA Australia recommends that the regulatory framework requires that all arrangements for the use of AI and ADM be subject to ongoing governance and assurance requirements, including

- the monitoring of performance on a continual basis, including for bias
- ongoing testing by multidisciplinary teams to ensure that the algorithms are working as intended and achieving the desired outcomes.

A 'risk-based approach' provides targeted regulation, allowing the community, businesses, governments and regulators to build trust and confidence in the use of these systems without imposing unnecessary burden on AI applications posing limited or minimal risk.

Recommendation 10:

Make the use of AI and ADM subject to ongoing governance, reporting and assurance requirements to ensure they remain lawful and up-to-date, and operate as intended.

Regulatory coordination

Whether there is evidence that poorly coordinated policy and regulatory activity in digital, data and cyber security areas have negatively affected businesses' investment, innovation or productivity?

It is not uncommon for businesses, that are (or want to be) involved in various government procurement projects, to be required to comply with multiple cyber security requirements. This can be costly, especially for SMEs, and creates a barrier to accessing government procurement contracts. Therefore, the government should aim to harmonise its cyber security requirements across the various government agencies and jurisdictions.

Furthermore, there is overlap, duplication and inconsistency in the regulation of AI and ADM. By way of example, if machine learning models need to be trained using data from different jurisdictions and sectors, different privacy laws apply. While those differences may be subtle, they nonetheless increase compliance costs for businesses.

Recommendation 11:

Harmonise regulation addressing digital, data and cyber security areas across different levels of government.

What policy issues and regulations are most important for agencies to coordinate on domestically and/or internationally, including both current and emerging areas?

Data sharing, data security and data privacy could benefit from harmonisation, similar to the approach by the EU through the GDPR. Privacy compliance can be challenging for Australian businesses who need to navigate the requirements of overseas jurisdictions, most notably the GDPR, to be considered a trustworthy recipient of personal information. Unless Australia becomes broadly regarded as providing 'adequate' privacy compliance, businesses will have to rely on their own capabilities and resources to navigate these legal and compliance burdens. Harmonisation would substantially streamline obligations for Australian businesses required to comply with the privacy laws of different jurisdictions, which would in turn enhance their participation in the global digital economy.

Another key element of a harmonised data security policy should be a whole-of-government approach to data security. Such an approach is important to ensure that a consistent approach is taken across government agencies. Data security requirements should not be dependent upon the department or portfolio in which the project is housed. Further, consistency in regulation would almost certainly support transparency for consumers and reduce compliance burdens on businesses.

Which policymakers and regulators must be involved to effectively coordinate government activity in digital, data and cyber security areas, and how should they be coordinated?

The Report refers to the Digital Platform Regulators Forum (DP-REG) to improve coordination on digital platform regulation between the ACCC, ACMA, OAIC and the Office of the eSafety Commissioner. How competition, consumer protection, privacy, online safety and data intersect (see DP-REG 2022), bears relevance not only for the listed regulators, but also for other regulators and policymakers.

For instance, the financial regulatory agencies, i.e., the Australian Prudential Regulation Authority (APRA), the Australian Securities and Investments Commission (ASIC), Commonwealth Treasury and the Reserve Bank of Australia (RBA) are currently working on, exploring and/or consulting on policy matters including e.g., digital payments systems, cybercrimes and scams, crypto-assets and others. These policy matters intersect with issues addressed by the DP-REG. The financial regulators are coordinated by the Council of Financial Regulators (CFR). We recommend that the DR-REG and CFR take a coordinated approach and work collaboratively on above-mentioned policy activities.

Furthermore, from an international stance, the Regional Committees of the International Organization of Securities Commissions (IOSCO) conduct annual Enforcement and Supervisory directors' symposiums. These symposiums allow regulators to discuss emerging trends, issues and policy initiatives that are being taken within jurisdictions and how they will impact the wider region. Coordination at this level should encourage harmonisation of standards across jurisdictions and greater cooperation and information sharing.

We note that the Department of Industry, Science and Resources is now responsible for national policy issues relating to the digital economy, the Department of Finance manages whole-of-government deregulation policy coordination, the Department of 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 between policymakers and regulators.

Recommendation 12:

Improve coordination between government entities and regulators and linking-up of digital economy policy development and consultation.