National Data Security Action Plan – Discussion Paper

Australian Capital Territory Government Submission

June 2022

Contents

Summary

The ACT Government welcomes the opportunity to provide this response to the *National Data Security Action Plan Discussion Paper* (the Discussion Paper).

Data is at the centre of enabling services and technologies that can improve outcomes for our community. Enhancing information and data sharing across all levels of government and with business is an enabler for more effective, efficient, accessible and equitable service delivery. Central to achieving this is continuing to safeguard the security and privacy of data as a valuable strategic asset.

The ACT Government recognises the increasing strategic, economic, and national security implications in how data is managed and is in-principle supportive of the proposal to establish consistent data security policy settings through a principles-based approach. This is a significant reform that will require a cooperative, planned approach to achieve uplift and complementary measures across all levels of government. In achieving consistency, it will be important for States and Territories to retain ownership of legislative and policy mechanisms that allow data and digital technologies to be used in innovative and nation-leading ways to improve the wellbeing and outcomes for our communities.

A reform of this scale requires whole of system thinking to be successful. The ACT is supportive of the intent of the Discussion Paper, however further discussions will be required to identify opportunities, impacts and constraints in the measures proposed in the Discussion Paper. The ACT looks forward to working closely with the Federal Government on the next steps.

ACT Government Data Landscape

The ACT Government provides and funds a wide range of services for and on behalf of the community, including education, health, housing, transport and roads, environment, business investment, and city and community services. The ACT Government also works with the Commonwealth, businesses and the community sector on service delivery and to achieve outcomes for the community.

Current ACT Government Data Landscape

ACT Legislation	Information Privacy Act 2014	Territory Privacy Principles (TPPs)
	Health Records (Privacy and Access) Act 1997	Territory Records Act 2002
	Children and Young People Act 2008	Freedom of Information Act 2016
	Human Rights Act 2004	Crimes (Sentencing) Act 2005
	Domestic Violence Agencies Act 1986	

		Overview
ACT Policy	ACT Protective Security Policy Framework	Provides ACT Government directorates and entities with a set of mandatory requirements to manage protective security risks.
	ACT Digital Strategy	Outlines the current and future initiatives that apply data to improve community wellbeing and the effectiveness and efficiency of government services.
	ACT Data Government and Management Framework and Guide	Sets out how the ACT Public Service will enhance its data practices for the benefit of the Canberra community.
	ACT Best Practice Design and Delivery Guide	A comprehensive guide to designing human-centered solutions for government programs and projects.
	ACT Risk Management Policy	Sets the minimum risk management standard expected of Territory entities in the management of risk.
	ACT Cyber Security Framework	The Cyber Security Framework, which has the *Cyber Security Policy* as its core, provides the policies, standards and guidance by which ACT Government secures our systems and

	data. It additionally includes the *Acceptable Use Policy* describing the requirements of staff to protect information assets, government functions and ICT Systems.

Strengthening data security

The ACT Government has invested in cyber and data security in response to the increasing security threat environment. Some examples of our actions include:

- Relocated critical capabilities from offshore providers to Australian data centres.
- Conducting our first ever whole of ACT government ICT Threat and Risk Assessment in 2020-21. The findings and recommendations are prioritised and form a program of work over several years to strengthen our security and resilience as a jurisdiction.
- Enhancing the distribution of national security information across government and increasing the number of security clearances for ACT Government personnel.
- Investing in the implementation of security information and event management capability.
- Work is underway to establish an ACT Government Cyber Security Centre.
- Invested in significant uplift in staffing dedicated to cyber security
- Uplift in hosting arrangements for more sensitive data (ensure not absolute statement)

The Digital Health Record

The ACT Government's Digital Health Record program will integrate health information from across the ACT public health system so healthcare professionals can access richer information about the patient and improve patient care. It will assist high-quality clinical decisions and motivate patients to participate in their healthcare.

The Discussion Paper

Alignment with international data protection and security frameworks (Q1)

As outlined in the Discussion Paper, the global data governance landscape is heavily fragmented and influenced by a range of legislative, trade and policy settings. National alignment would be supported by complementary data protection and security settings between the Commonwealth and State and Territory governments. Consistency in national data flows would support consistency in future bilateral and multilateral agreements involving Australian data.

Commonwealth support to uplift data security across governments, businesses and community (Q3/10/14)

We view that there are a range of activities the Commonwealth can lead or enhance to support governments and businesses to meet a principles-based approach to data security.

Communication campaigns, education and awareness

- Increase communication and education campaigns to raise awareness of cyber threats and actions individuals should be taking to protect their personal and financial information.

    - *The Australian Cyber Security Centre (ACSC) and Australian Federal Police provide education and awareness campaigns.*
        - *Consider research into differences in attitudes across demographics and target campaigns to different cohorts (young people/seniors) that measure behavioural change to understand what works best.*
        - *Consider the role of the Commonwealth in providing education and awareness raising and responses to fake news and communications – a 'point of truth'.*
    - *States and Territories could reinforce key messages through their own communications and engagement channels if the collateral was shared.*

Technology

- Work with global technology leaders and Software as a Service providers to increase awareness on the minimum security standards expected by governments, once agreed.
    - *The implementation of vaccination certificates is an example of how consistent security settings would support national outcomes. While there was variation in how the state-based check in apps handled the vaccination certificates, State and Territory Check-In app solutions were more tamper-proof than a download to a commercial wallet.*
    - *The recently released Human Rights Watch report revealed a range of education technology products widely used in schools had the capacity to monitor children, engaging in data practices that put children's rights at risk.*

Identity

- There is opportunity through this action plan to join up the identity system in Australia in ways that make it easy and intuitive for people to access government services while improving the integrity and protections of their identity information. All areas of the Commonwealth with a remit in this area could work to ensure that Australia is doing everything possible to create, protect and safeguard the identity information of our citizens and businesses.
- Digital identity is part of this ecosystem. It relies on identity created and verified in states and territories through the health system, Births Deaths and Marriages agencies, drivers' licences, and Commonwealth managed passports.
- The integrity of the identity creation, and proof of identity processes is an essential part of the trust chain, as is ensuring that there are appropriate prevention and detection mechanisms in place alert to compromise and misuse.
- Consider evolving the identity capabilities to reduce the number of times individuals are required to provide their identity information through data sharing between trusted parties.
    - *This should include change of name or gender markers to allow individuals to easily access proof of identity documents that match their current status.*
- Consider how we move from identity verification at a point in time, to monitoring digital identity in use as a key strategy in the fight against identity theft and cybercrime more generally.
- We stress the importance of governments working together to support victims of identity crime. Currently victims are referred and provided advice about how they can go about restoring their own identity in the community, and commence the process to re-establish who they are with each agency and level of government. Consider a national approach to supporting victims of identity crime.

Building the cyber workforce

- Work with States and Territories and higher education providers to ensure investment in the cyber curriculum delivers measurable outcomes in the form of work-ready graduates that are employable at government standards.
    - *The partnership between the Australian Signals Directorate and the Australian National University is one example.*
    - *The REDSPICE blueprint presents an opportunity to set a national plan for the higher education cyber curriculum Australia requires to meet our cyber security needs across the Commonwealth and States and Territories.*

AGVSA

- An increased focus on data security will put further pressure on an agency struggling to achieve timely vetting of personnel. Consider investment in AGSVA in anticipation of further demand.
    - *The timeframe for security clearances has resulted in the ACT Government establishing its own security vetting process to induct personnel in a timely manner.*
    - *Consistency in data security settings should be matched by the option for governments to access a consistent standard of security vetting led by the Commonwealth.*
    - *Higher demand for security vetting is anticipated, and further delays will have flow-on effects for the implementation of national initiatives.*

Data localisation (Q5)

The ACT Government is supportive of data localisation for governments and critical infrastructure providers.

However, it is also important that data localisation is accompanied by measures that encourage businesses to invest in new and emerging technologies within Australia. In the past, concerns and uncertainty on data sovereignty have resulted in extensive delays and significantly higher costs to government to implement new technologies readily available in other countries. We view that a nationally-consistent risk-based approach to data localisation would support agility in introducing systems and services that improve outcomes in the community.

Harmonising data security policy between all jurisdictions (Q6/7)

The ACT Government supports the proposal in the Discussion Paper to establish consistency in data security settings between all jurisdictions. It is important that jurisdictions work together to respond to current national security challenges and protect our critical data as strategic assets of local and national significance. The COVID-19 pandemic has repeatedly demonstrated the benefits of a joined-up approach to tackling matters of national importance, such as the work of Data and Digital Ministers to support the implementation of vaccination certificates in Check-In Apps across States and Territories.

To further this objective, it will be important for the Commonwealth to also adopt a whole of government approach that would support States and Territories to consider complementary reforms. While the Discussion Paper attempts to align various Commonwealth initiatives, we view that the following require further consideration:

Intersection with digital identity reforms

- Digital identity reforms form part of the broader ecosystem of the Discussion Paper and is an important vector to achieving this objective.
    - *The role of the Digital Transformation Agency's Trusted Digital Identity Framework in the national data security landscape should be clarified.*

    - *Consider a single policy mechanism for identity proofing and digital identity verification.*
    - *A future national digital identity capability should:*
        - *consider the end to end of the trust chain to safeguard against cyber threats*
        - *maintain integrity and assurance in proof of identity processes from creation to retirement, including original identity documents created by States and Territories.*

Accelerate the objectives of the *Intergovernmental Agreement on Data Sharing (Data Sharing IGA)*

- The Data Sharing IGA will remove barriers between jurisdictions when they share data. The Data and Digital Minister's associated work program demonstrates how jurisdictions can use the Data Sharing IGA. However, there are costs associated with sharing data that may prevent some jurisdictions, especially smaller jurisdictions, from benefiting from this work. Jurisdictions will need to careful balance cost recovery activities with the benefits of greater data flows when considering how they will resource data sharing activities.
- Investment in the design and delivery of the governance and foundations of a whole of nation data sharing capability would support this objective.
- The National Disability Data Asset (NDDA Pilot) was finalised on 31 December 2021. The objective was to progress people-centred data sharing across jurisdictions at scale, focused on understanding outcomes of people with disability (one in six Australians). The success of this pilot demonstrates the ability to create an infrastructure, data and linked asset to provide insights on people in Australia, and that this could be built out to be an Integrated Data Infrastructure for people centred information for people in Australia.

Alignment with the review of the *Privacy Act 1988* (Cth)

- The management of data is closely linked to legislative privacy settings at both the Commonwealth and State and Territory levels.
    - *The Attorney-General's Department review of the Privacy Act 1988 (Cth) is still underway. It will be important for the outcomes of this review to be considered in the context of this objective due to the potential flow-on impacts to State and Territory privacy legislation and policy settings.*
        - *The impact of this review on the ACT Information Privacy Act 2014 is unclear and will need to be assessed.*
    - *Consideration of international regulatory standards, such as the European Union's General Data Protection Regulation, should await the outcomes of this review.*

Whole of system approach

- While the Discussion Paper is primarily focussed on preventing deliberate incursions from malicious actors, the data security pillars should be equally cognisant of accidental or inadvertent loss, damage or alteration of data through inadequate system design.
- In addition, the value, importance and sensitivity of data, and therefore the designation of appropriate standards for their protection, can have a wide variety of contexts. Data holders should be encouraged to have a broad understanding of the value of their data. High levels of protection may be required to protect data with narrow, short term value, so as for day-to-day business continuity, or for community-wide, long-term value such as for the national memory and cultural heritage of Australia as a whole

The Commonwealth has the option to lead the development of consistent data standards and invest in building scalable central capabilities that States and Territories can leverage to implement national initiatives that require data sharing. When Commonwealth requires jurisdictions to support national initiatives such as NDIS worker screening, Automatic Mutual Recognition of Licencing and Registration, it could lead the work on data standards and invest in building the central capability that all jurisdictions can leverage to facilitate data sharing.

Consider leveraging and uplifting capabilities such as the data exchange being developed by Services Australia for the Birth of a Child Program. This program aims to reduce the burden on parents to register their newborns in a range of government services, and establish an identity of integrity that we can all rely on. The pilot is expected to be complete by end of the 2022 calendar year. The central, national capability will have been built, and jurisdiction onboarding as part of a national rollout will contain the financial investment to connecting their systems and adjusting their own processes.

Achieving consistency and uplift – A cooperative reform model

Achieving the objectives outlined in the Discussion Paper requires cooperative reform between the Federal and State and Territory governments. Currently, there is no identified Ministerial council to provide oversight and national direction to the National Data Security Action Plan as a Commonwealth document. We view that this is an important measure to ensure there is national support and agreement on uplifting data security standards.

ACT Government support

The ACT Government has identified the following measures to support consistent data security policy settings, some of which are already under consideration:

- Promote and distribute Commonwealth communication, education, and awareness collateral on protecting personal and sensitive information through our service delivery (schools, community services, economic development initiatives).
- Consider alignment of the forthcoming *ACT Protective Security Framework* to the *Commonwealth's Protective Security Policy Framework* (PSPF) to support a common minimum standard to the extent practicable.
    - The ACT recognises the benefits of alignment with the Commonwealth PSPF to support consistency in information, personnel and physical settings that can enhance collaboration and sharing between jurisdictions.
        - *There are practical limitations and barriers to alignment for the ACT, in particular the employment of permanent residents and non-Australian citizens.*
        - *There is a significant cost in alignment with Policy 8: Sensitive and Classified Information of the PSPF to create and maintain PROTECTED enclaves that also presents a barrier to alignment.*
- Incorporate minimum security standards into all ICT procurement documents.
- The ACT Government is the lead jurisdiction for the Birth of a Child program and continues to engage state and territory agencies in the design and delivery of the program, in close partnership with Services Australia.