Northern Territory Government Submission

National Data Security Action Plan Discussion Paper

NORTHERN TERRITORY GOVERNMENT

Acronyms	Full form
ACSC	Australian Cyber Security Centre
CALD	Culturally and linguistically diverse
CCNT	Chamber of Commerce NT
CTH	Commonwealth
DAWG	National Data Analytics Working Group
DCDD	Department of Corporate and Digital Development
GDRP	European Union's General Data Protection Regulation
IGA	Intergovernmental Agreement
JCSC	Joint Cyber Security Centre
LGANT	Local Government Association of the NT
NT	Northern Territory
NTG	Northern Territory Government
PII	Personally identifiable information
SOCI	Security of Critical Infrastructure Act
SMEs	Small to Medium Businesses

Contents

Overview

The Northern Territory Government (NTG) recognises the value of data to governments, organisations and businesses in Australia and that citizens expect that their data is secure and protected.

The NTG supports the intent of the *National Data Security Action Plan* to establish a national and proportionate standard for the protection of data across the economy, underpinned by three principles for data security: secure, accountable and controlled.

The NTG recognises the steps the Australian Government is taking to seek to align the *National Data Security Action Plan* in the broader context of the digital economy, national data strategy and other digital government transformation priorities. The principles and governance which guide and protect data assets should ensure that sensitive data is afforded the highest level of protection while at the same time there is transparency about the use of citizen data, consistent with the Trust Principles previously agreed by Data and Digital Ministers across all Australian governments.

The NTG has considered each of the 'call for views' questions in the discussion paper and provided a summarised response against each of the four main groups of issues:

- Common understanding
- Governments' role
- Clarity and empowerment for businesses
- Empowering and educating citizens and consumers

This submission also provides observations on the anticipated challenges to achieving a national approach in the areas of local government and across small and medium enterprises in the Northern Territory.

The NT Department of Corporate and Digital Development (DCDD) works closely with the Local Government Association of the NT (LGANT) and the NT Chamber of Commerce (NTCC) to promote cyber security awareness and practice in these sectors.

DCDD provides cyber security services to NTG agencies and represents the NT Government on the National Cyber Security Committee and associated sub-committees; works in partnership with the Australian Cyber Security Centre (ACSC) and leads data security policy, representing the NTG at the Data and Digital Ministerial Council. DCDD also engages with private sector entities on data storage initiatives in the Northern Territory.

It must be noted that organisations across the broader economy will be challenged in obtaining professional ICT services to implement the National Data Security Plan in a skill shortage environment, adding increased costs, particularly in an environment where multiple Australian Government security initiatives are being implemented or considered, including the *Security of Critical Infrastructure Act* (SOCI). Practical and tailored guidance and toolsets will be critical to supporting organisations to meet compliance requirements and achieve the intent of the National Data Security Plan.

Common understanding

National Harmonisation

Implementing a proportionate National standard for data protection is supported.

The discussion paper identifies many of the complexities of the international environment which provide challenges and opportunities for Australian governments and businesses. One of the key challenges is the diversity of approaches to data regulation and data protection globally.

There is merit in Australia adopting a national framework to inform international data sharing agreements and industry practice. Alignment to the European Union's General Data Protection Regulation (GDPR) is sensible, however this is recognised as a significant uplift in security standards, particularly for the small business sector. This sector is presently excluded from having to comply with the Privacy Act and Notifiable Data Breach Scheme and extending data protection regulation to this sector may require financial support, noting the considerable costs to organisations to implement data security solutions, processes and staff training.

Comprehensive multi-media education campaigns, developed in partnership with industry groups and financial incentives to support organisations to understand future legislated data security requirements will be required to support adoption. Education will be imperative to supporting this sector to be aware of new data security standards and its ability to comply. It is anticipated organisations will seek advice from the Australian Government in the form of supporting guidelines, toolsets and training to assist them to meet new data security standards. The Australian Government may also consider a staggered approach to applying punitive measures.

The NTG advises that organisations and businesses in the Northern Territory required to implement national data security standards will be significantly disadvantaged by the absence of a JCSC in Darwin.

Proportionate data protection

Personally Identifiable Information (PII) data is most sensitive to citizens, yet the management of PII is not fully regulated across the economy.

National security and critical infrastructure data is most sensitive and presently regulated under the *Security of Critical Infrastructure Act* (SOCI) and Protective Security Policy Framework.

The SOCI identifies data storage and processing providers as critical infrastructure where servicing a Commonwealth, State or Territory Government or an entity responsible for a critical infrastructure asset.

The Act establishes positive security obligations and a risk management approach to protecting critical infrastructure assets across a range of hazards, including supply chain risk.

A National data standard should apply a similar risk based approach to identifying the data type, data life cycle and impact of compromise to the confidentiality, integrity and availability

of the data to define proportionate data security controls and policy. Supporting guidelines should aim to support small to medium enterprises to consider data collection appropriate to business purposes that accords with cyber security controls in order to minimise risk.

The NTG supports proportionate data security standards that recognises data associated with national security and critical infrastructure, and personally identifiable information as the most sensitive.

The NTG supports incorporating a risk management approach within a National Data Security Standard.

International data sharing

Recognising the complexity and variety of international approaches, there would be considerable value in the Australian Government providing guidance that can efficiently highlight issues in particular jurisdictions (ie country-level guidance) as well as role based guidance (eg for export businesses, offshoring of services, or for citizen protections).

Localised data storage

Cloud based services pose challenges in enforcing data sovereignty requirements in the absence of national legislative requirements.

It would be of benefit for all Australian governments to review the risks and benefits of emerging data storage models (including offshore hosting) in a more nuanced way. There may be national commercial benefits in exploring reciprocal hosting arrangements between sovereign governments. Under such arrangements associated risks must be considered and balanced with appropriate trust and legal protections in place, guided by nationally consistent frameworks for risk management and security controls.

Similarly, regulating on-shore data storage for certain data, such as PII may drive further investment in Australia's digital economy. The NTG is actively seeking private investors to develop and operate data centres in Darwin in recognition that data centres require and support growing digital skills and foster opportunities to develop digital technology and advanced manufacturing.

In addition, regulating transparency in data storage and transmission will aid organisations to manage supply chain risk.

In considering localised data storage requirements the Australian Government may consider the capacity of the private sector to respond and design a staggered approach to such requirements.

The NTG supports the Digital Transformation Agency's Hosting Certification Framework but notes the compliance requirements can lead to market consolidation and add to concerns about data centralisation. The paper's reference to managing redundancy risk is also acknowledged by the NTG. Applying sound risk management approaches requires building redundancy into data storage management.

Harmonisation with cyber security regulations

The Australian Government's discussion paper**,** *Strengthening Australia's cyber security regulations and incentives*, similarly seeks to achieve a whole of economy uplift in cyber security with proposed minimum standards for personal information via an enforceable cyber security code, and minimum governance standards for large business to manage protecting personal information and cyber security risks. This paper proposed options including mandatory governance standards for large businesses that can be voluntarily applicable to smaller businesses. It is noted that an uplift would require considerable time to be applied and would add cost in the areas of governance, security controls and awareness, with costs likely to be passed on to consumers.

This paper commented on the current Review of the Privacy Act considering the connection between cyber security and the protection of personal information.

Aligning the outcomes of the *Strengthening Australia's cyber security regulations and incentives Discussion Paper*, Review of the Privacy Act and potential development of a cyber security code, and the *National Data Security Action Plan* will aid governments' endeavours to reduce the risk of regulatory overburden. Developing an overarching regulation matrix tool, that articulates where measures are scalable or mandatory to data type, will assist organisations to interpret and adopt the appropriate regulatory measures to their organisation. The toolset could also detail other regulatory requirements, including under the *Security of Critical Infrastructure Act* (SOCI) and associated standards, to assist organisations, including those in the supply chain.

Government's role

Policy alignment

The Data and Digital Ministers spearhead cross-jurisdiction collaboration on matters relating to data policy and government digital transformation. Similarly, committees of senior officials and technical experts exist in the cyber security and data sharing environments. The NTG considers these groups to be an effective vehicle to further the harmonisation of data security policy across jurisdictions. The groups would be aided by a national funding framework, particularly to implement data security and legislative reforms in a timeline aligned to the National Data Security Plan.

All jurisdictions have differing legislative positions on data management. For example, South Australia has data sharing legislation but defaults to the Commonwealth Privacy Act whereas the NT has modified the principles from the (Cwth) Privacy Act and imbedded these into Information Privacy Principles under the (NT) Information Act.

Additionally, requirements for Privacy Impact Assessments differ between jurisdictions which results in multiple agreements to share data across jurisdictions.

Harmonisation of data security policy across jurisdictions is challenging and will need significant investment to align legislative and policy settings. The Data Sharing Agreement template and approach established by the Office of the National Data Commissioner provides a model for national adoption alongside adopting existing national policy elements including the Five Safes Framework and Trust Principles.

Examples of activities within these groups relevant to data security standards includes:

Data sharing within Australian Governments

The National Data Analytics Working Group (DAWG), formed under the Digital and Data Ministers Meeting, is progressing oversight on a number of data sharing projects under the Intergovernmental Agreement (IGA) on data sharing that was signed by the Prime Minister and state and territory First Ministers on 9 July 2021.

Jurisdictions have committed to participating but are citing financial and resourcing constraints that are impacting participation in the IGA.

The absence of national data sharing arrangements and secure platforms are a present challenge for all governments.

Identity Resilience

DCDD participates in the National Resilience Working Group, formed under the Digital and Data Ministers Meeting, which is tasked with developing a functional model of Identity Resilience and considering nationally consistent legal frameworks.

Smaller jurisdictions like the Northern Territory face the challenge of limited financial capacity and limited personnel resources to enact system and regulatory changes, particularly the replacement of legacy systems.

The Australian Government may consider the establishment of a senior level working group compromised of representation by all jurisdictions, with a specific terms of reference to improve data security policy alignment and legislative harmonisation between jurisdictions and to identify the barriers, including estimated costs to implement and associated resourcing and funding, and opportunities to achieving this aim. Jurisdictional representation will enable the states and territories to consider potential impacts of national legislative changes on local arrangements.

The NTG supports establishment of a senior level working group to improve data security policy alignment and legislative harmonisation between jurisdictions and inform implementation of the National Data Security Plan.

Promotion of regulation

Governments have a role in promoting compliance to legislation. The introduction of new national regulations or legislation should be supported by national awareness activities targeted at organisations to build awareness of regulatory obligations and for citizens and consumers on best practice principles.

Local Government

There are 17 local government councils in the Northern Territory servicing urban and remote areas. Each local government council manages PII of Northern Territory citizens. Local Government organisations do not provide water and electricity, which are provided by the Northern Territory Government, and thereby as entities are not affected by SOCI.

DCDD engages with local government entities on cyber security matters and notes a wide range of maturity, awareness and prioritisation of cyber security across local government organisations.

Access to specialist and technical services to local government organisations, particularly in remote areas can be limited by the availability of professional services, remoteness and funding at the council level.

Extending regulation of data security to local government entities across Australia will require additional substantial investment in cyber security and data security, likely to be passed on to consumers in the absence of national investment.

The NTG supports the responsibility for managing local government data security remaining with local government organisations. Data security management requires policy and practices to be applied within the business functions of a local government organisation and cannot be managed through cyber security controls alone or by an external body.

In line with recognising the scope of PII held by local government as a collective, the sensitivity of PII as a data set, and the limited own-source revenue raising capacity of smaller Councils, the NTG would support a federal funding package and ACSC led practical support, such as a Council Cyber Security Uplift program, to support local government organisations to comply with new data security regulation.

The NTG supports the responsibility for managing local government data security remaining with local government organisations.

The NTG would support a federal funding package and ACSC led practical support, such as a Council Cyber Security Uplift program, to support local government organisations to comply with new data security regulation.

Clarity and empowerment for Business

Small businesses are particularly vulnerable to cyber security threats and the potential compromise of PII, commercially sensitive information and business disruption. DCDD engages with businesses and industry groups across the Northern Territory on cyber security awareness and finds low cyber security awareness and maturity, consistent with the ACSC Small Business Survey (2020).

Extending and mandating data security standards and data breach notification to small and medium businesses represents a significant step-up in regulation with direct impacts on business systems, business processes and internal governance and risk management and business costs. The NTG would support identifying anticipated implementation costs for SMEs and Federal support incentives and programs to assist businesses to comply.

The NTG also recognises that regulation should be commensurate with risk. In the context of the wide variance of businesses and sectors across the SME environment, SMEs would be supported by industry specific guidance to assist organisations to identify the type and commensurate value of data, applicable regulations, and guidance on risk assessment.

Consistent with the section above regarding harmonisation with cyber security regulations, the NTG would support developing a regulation matrix tool to assist organisations to comply. A

tool that articulates where measures are scalable or mandatory to data type, will assist organisations to interpret and adopt the appropriate regulatory measures to their organisation.

The introduction of new national data standards and application to new sectors, such as small and medium business will require national awareness activities targeted at affected sectors.

Direct Government communication to SMEs and partnering with industry groups to aid promotion is critically important to driving awareness of both regulations and available government advice to support compliance.

Communication mechanisms through JCSCs, Federal and State agencies and government business programs, including the Australian Tax Office and state-level business agencies are well placed to support nationally coordinated data security awareness activities.

The NTG would support the Australian Government identifying anticipated implementation costs for SMEs and Federal support incentives and programs to assist businesses to comply, including the provision of industry specific guidance and communication and awareness activities.

Empowering and educating citizens and the community

The NTG has not canvassed the views of individuals in its response to this call for views. However, it has explored related issues of privacy, digital inclusion, trust in government and cyber security in related community engagements.

One of the central roles of governments is community protection, particularly the protection of our most vulnerable. Securing private and personal data of citizens held by governments is paramount not only because it is the government's role, but also to build community trust in data and digital technologies, which in turn enables more government services to be delivered more effectively using the data assets entrusted to us.

It is essential that citizens and consumers understand their rights. The previously mentioned Trust Principles, augmented with consumer data protection principles modified from the GDPR and communicated effectively will support increasing citizens' awareness and expectations of data security.

Specific to the Northern Territory is a large cohort of First Nations communities for whom English is a second or third language. National communication activities on data security should include culturally-appropriate communication activities targeted at First Nations communities, and culturally and linguistically diverse (CALD) communities.

The NTG supports integration of the Trust Principles in the National Data Security Plan and community communication initiatives to increase awareness of data security expectations.

The NTG recommends national communication activities targeted at citizens to increase awareness of data security expectations includes a focus on First Nations and CALD communities.

Concluding Remarks

In addition to the specific issues and observations noted above, the NTG would like to highlight the following general issues:

- Trust Principles have been agreed by all Australian governments and are relevant to underpinning the National Data Security Plan. The NTG would support the integration and reference to the Trust Principles in the Plan.
- Striking a balance between security and accessibility is crucial to the success of any data security initiative. In a similar vein, a pragmatic approach to enacting data protection principles will aid acceptance and compliance by organisations holding data on citizens.
- The notion of the 'right to be forgotten' should be a central commitment for citizens, promoting trust and providing choice.
- Privacy and Information legislation across jurisdictions can benefit from closer alignment and, in some cases, modernisation, to recognise the rapid evolution of the information/data management environment.
- The National Data Security Plan will require implementation planning, and should identify implementation cost estimates for SMEs and governments. Equally for SMEs and jurisdictions with limited resources, there needs to be certainty about the cost and funding by the Australian Government to drive whole of economy uplift, as well as some detail about timing of outcomes and resource requirements.
- Technology continues to change and although it is not possible to future-proof any national system, the National Data Security Plan should recognise the continuous advances in data security and related fields (such as artificial intelligence, machine learning and quantum computing) and account for such changes.

The Northern Territory Government continues to actively participate in cross-jurisdictional groups and welcomes the opportunity for further collaboration to explore the issues and implementation planning, including designing a national data security system that will meet the needs of all Australians.