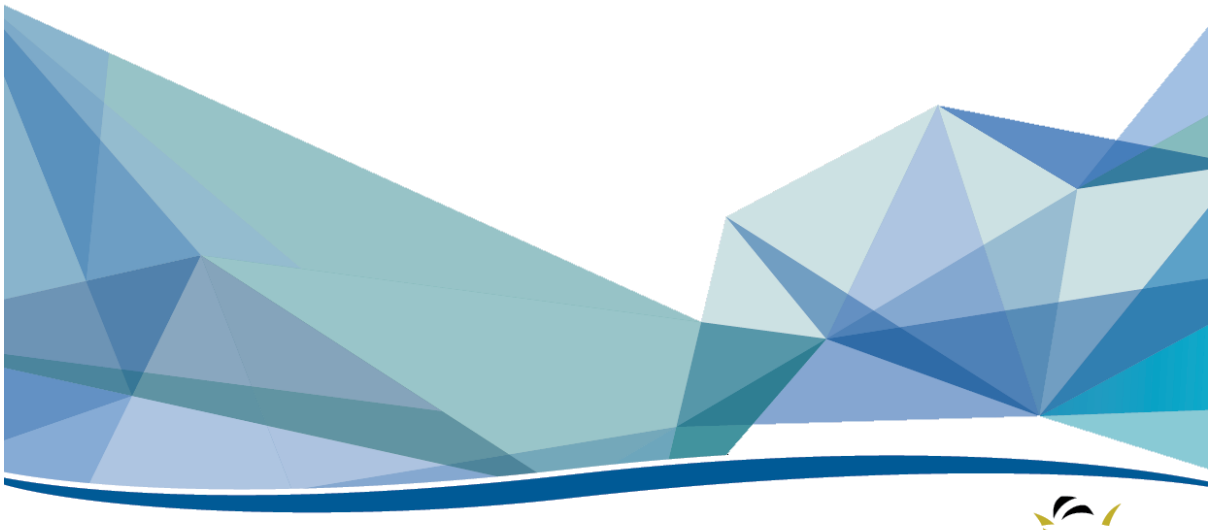
Tasmanian Government Submission

National Data Security Action Plan discussion paper
May 2022



Tasmanian Government

GLOSSARY

ACCC	Australian Competition and Consumer Commission
ACSC	Australian Cyber Security Centre
ACS	Australian Computer Society
ASD	Australian Signals Directorate
Blue Tech	Digital Trades (technology-intensive jobs requiring sub-degree level qualifications), which are best met through the TAFE education model
Cwlth PSPF	Commonwealth Protective Security Policy Framework
DATA Scheme	Data Availability and Transparency Act 2022 Scheme
EU	European Union
FTE	Full Time Equivalent
GDPR	General Data Protection Regulation
GDSI	Global Data Security Initiative
IGA	Inter-Government Agreement
IOS	(previously named iPhone OS) is an operating system for mobile devices, made and sold by Apple Inc.
ISO/IEC 20000	International standard for IT service management
ISO 27001	International standard for the requirements of an Information Security Management System (ISMS)
ISO 27040	International standard for information storage system security
ISM	Information Security Management
IRAP	Infosec Registered Assessors Program (IRAP)
NDB	OAIC's Notifiable Data Breach Scheme
NIST	National Institute of Standards and Technology
OAIC	Office of the Australian Information Commissioner
ONDC	Office of the National Data Commissioner
Para-professional	A person to whom a particular aspect of a professional task is delegated but who is not licensed to practise as a fully qualified professional. In the context of ICT, engineering and construction, para-professional qualifications are Certificate IV to Advanced Diploma.[1]
PII	Personally Identifiable Information
PSPF	Protective Security Policy Framework
SEE Learning Program	Skills for Education and Employment (SEE) program https://www.dese.gov.au/skills-education-and-employment
SMEs	Small to medium sized businesses
SOC 2	System and Organisation Controls is a comprehensive reporting framework put forth by the American Institute of Certified Public Accountants (AICPA) in which independent, third-party auditors (i.e., CPA's) for an assessment and subsequent testing of controls relating to the Trust Services Criteria (TSC) of Security, Availability, Processing Integrity, Confidentiality or Privacy. **It** is both an audit procedure and criteria. It's geared for technology-based companies and third-party service providers which store customers' data in the cloud. SOC2 is one of three types of reports. Companies used to comply with SOC 1 only, but as companies moved to cloud-based storage, they also target SOC 2. SOC 3 report is for public use.
SOCI Act	Security of Critical Infrastructure Act 2018
TPSPF	Tasmanian Government Protective Security Policy Framework
TSS	Tasmanian State Service

[1] Civil Construction Industry Workforce Plan 2019-2025. Workforce Plan Template (skills.tas.gov.au)
Workforce Development Plan 2016-2019. Engineers_Australia_-_Tasmanian_Workforce_Development_Plan_2016-2019.pdf (skills.tas.gov.au)

1. INTRODUCTION

The Tasmanian Government welcomes the opportunity to make a submission on the *National Data Security Action Plan (The Action Plan)* discussion paper. The Tasmanian Government supports the high-level principles as it aligns with the economic focus area in the Tasmanian Government's *Our Digital Future* strategy. Tasmanian Government sees data security as an enabler for thriving digital economy. The Tasmanian Government supports the linkages of data security with critical infrastructure in the action plan.

This submission raises some specific matters that the Tasmanian Government believes should be considered when seeking to improve data security measures for all levels of government and business in Australia.

To address information security for consumers and businesses, and actions the Australian Government can take, the Tasmanian Government makes the following observations:

- Inconsistency of Standards. The inconsistency in standards for assessing and handling sensitive government data holdings has been identified and addressed in part through development of the Tasmanian Government Protective Security Policy Framework (PSPF). There is an opportunity for Australia to better align with international frameworks by utilising case studies such as New Zealand whose data security standards were accepted by the European Union (EU). This information could be shared under the Intergovernmental Agreement (IGA) for data sharing.
- Security Risks and Responsibilities of Third-party Suppliers. More focused work is needed to manage the security risks associated with third-party suppliers. While there are standards that can be applied to the information security management such as ISO 27000 family, there is limited legal requirements that compel their use. Generally, these matters are managed as part of individual contractual arrangements with vendors and agreed on a case-by-case basis. The onus falls on the customer to mitigate or accept the risk to ensure an appropriate level of security. If the intention is to extend this Action Plan to local government and general consumer transactions, a staged plan of education and scaled implementation should be a high priority to protect these most vulnerable users. It should also be supported by a national certification process to lift consumer confidence in identifying credible data security products.
- Awareness and Education. A Data security awareness and training campaign is needed to target critical infrastructure and small businesses. It is critical to uplift data security awareness and capability for all levels of government and all sized businesses. The awareness campaign needs to start with the individual and placing greater value on their own data before handing it over to government or private businesses, and then extending this to supply chain participants such as private businesses/vendors/suppliers and clients, and highlighting the risks, roles and responsibilities. One approach could be a campaign directed to consumers and small, low-tech businesses to inform and illustrate ways in which valuable data is harvested in small increments but becomes significant when consolidated.
- Critical Infrastructure Workforce Development. Specific targeted engagement with all new critical infrastructure asset owners and responsible entities captured under the Security of Critical Infrastructure Act 2018 (SOCI Act) reforms by the Australian Cyber Security Centre (ACSC) and the Cyber and Infrastructure Centre on data security and new cyber security obligations should occur as soon as possible.
- Cyber Security and Data analytics Skills Shortage. Skills shortage in cyber security and data analytics was lightly touched on in the Action Plan but is a major factor impacting all levels of government and the business sector in their ability to effectively achieve the level of change required to ensure improved national data security. Targeted professional development, education and training in early and mid-career ICT/Cyber professionals is warranted to build a pool of critical expertise. A modified version of the harvesting campaign mentioned above could be delivered to non-ICT government staff as a core training unit to raise awareness of cyber security alongside more general privacy obligations.

2. TASMANIAN CONTEXT

The Tasmanian Government's *Our Digital Future strategy* aligns with the Australian Government's commitment to make Australia a top 10 digital economy by 2030. The Tasmanian Government is also committed to the harmonisation of security classification systems and is informed by the Commonwealth PSPF in the co-design and development of the Tasmanian PSPF.

By integrating the *Action Plan* with *Our Digital Future* and aligning with future national data security requirements, Tasmanian Government will be well placed to:

- ensure that public data held by Tasmanian State Service (TSS) agencies is securely transmitted and stored, providing confidence to local business and the greater community relying on TSS services.
- Provide guidance and support to Tasmanian business on their security obligations when using, transmitting, or storing both commercial and personal data.

There are a broad range of factors that currently prevent the adoption of a whole-of-economy approach to data security in Australia and are outlined below against the three focus areas of the *Our Digital Future* strategy:

Factors/Focus Areas	Our Digital Community	Our Digital Economy	Our Digital Government
Inconsistency of standards	✓	✓	✓
Increasing obligations and expectations across public and private sectors		✓	✓
Critical Infrastructure Workforce		✓	✓
Cyber security and data analytics skills shortage		✓	✓

Inconsistency of standards.

- The lack of a national framework that is aligned with best practice international frameworks such as the EU.
- Numerous and complex security standards.
- Cost and resourcing required to implement data security frameworks.
- Lack of commercial incentive for businesses to implement measures and frameworks.

Increasing obligations and expectations across public and private sectors

- There is increasing obligations and expectations across both public and private sectors, which many smaller businesses and governments are not able to adequately fund. The Tasmanian Government, as a small jurisdiction with limited resources, experiences this issue as the community has expectations that Government will provide the same level of service as the larger jurisdictions.

Critical Infrastructure Workforce.

- Data security literacy and skills is a gap for critical infrastructure asset owners and small businesses.
- Critical infrastructure is significant for Tasmania and is supported by a blue tech workforce of para-professionals and small businesses.
- 98% of businesses in Tasmania are classified as small businesses.
- Para-professional careers in energy, water and building construction evolve into small businesses where project, data and information management increasingly becomes a core element of the business.
- Para-professionals draw on digital literacy and project management skills gained through their vocational experience, education and training[1]. However, data management and security skill sets are often absent in formal vocational, education and training curriculum.

Cyber security and data analytics skills shortage.
The national ICT/Cyber skills shortage is even more acutely felt by employers in the areas of cyber security and data analytics. There is a need for targeted professional development, training and education to develop the workforce with expertise to support government and business to effectively achieve the level of change required to ensure improved national data security.

3. BUILDING A COMMON UNDERSTANDING

1. What do you consider are some of the international barriers to data security uplift?

The lack of a unified approach at the international level is a key factor that creates barriers to uplifting data security and drives regional approaches that lack the transparency, security and regulatory provisions with respect to where and how data is stored and managed.

For example, given that Australia is not included in the list of countries aligned with the EU's General Data Protection Regulation (GDPR), it is interpreted that Australia's data security standards are not on par with EU standards. Without both identifying and complying with an agreed international standard, Australia will face difficulties in engaging on international data security and achieving the desired security outcomes it is seeking.

Global regions tend to focus on their own economic needs and political agenda without considering the wider global picture, and their local laws on data management and security can lack acceptable incident reporting and limited legal recourse if an incident such as a data breach was to occur.

This causes fragmentation and distrust preventing a truly international policy on data security. Instead, jurisdictions implement complex protections that benefit litigators more than consumers. For example:

- The EU has the GDPR that is tailored to protect the data of EU citizens globally and highly punitive laws exist.
- China has the Global Data Security Initiative (GDSI). The GDSI has gained general support from countries like Russia, Tanzania, Pakistan, Ecuador the Arab League and ASEAN countries.
- The United States, by contrast, does not have a single principal data protection legislation, relying rather on hundreds of federal and state laws aimed at protecting data of US residents.

International law does not provide adequate protection for victims of data theft or corruption. End user licensing agreements are written to limit the liability of software providers, leaving users with significantly restricted options for redress. Private international law – actions between non-state parties – provides still less protection for Australian victims of data crimes because judgements cannot be enforced effectively against off-shore offenders.

Many cloud-based service providers do not offer Australian based services due to the lack of economic return on investment. For suppliers, it becomes a trade-off between data security versus access to the service/function that is needed by the consumer.

Unlike these jurisdictions, Australia does not currently have the resources or the scale of operations to warrant multiple data security standards. The best protection for Australian interests is to promote a more streamlined system of engagement. The ideal is a set of legislation and standards that provide clarity, confidence and promotes the benefits for small stakeholders who are at greatest risk of a data breach.

2. How can Australian Government guidance 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)?

The EU's GDPR framework would appear to be a good benchmark for Australia to pursue. The GDPR sets a standard to aim towards and could perhaps be adapted to meet the requirements of the Australian public and local context, as part of any intended maturity roadmap.

This legislation and its associated obligations provide recourse to individuals in the event of loss or theft of their data.

There has been precedence set where international alliances and agreements have been achieved that Australia could adopt. This would enable Australian data to be managed according to Australian law while using cloud storage facilities in other countries. For example, for US vendors offering cloud storage within the US to Australian businesses could be managed by an agreement, similar in intent to the US GDPR Data Shield agreement, might mean that Australian data are managed according to Australian law and not subject to US Law such as the PATRIOT act when stored on behalf of Australian custodians but within US data centres. (NOTE – Courts have ruled that the Data Shield Agreement does not meet the GDPR requirements for the transfer of data from the EU to the US).

Harmonisation, however, would pose challenges due to the potential impacts on existing associated and underpinning laws, acts, policies and guidelines across all Australian governments. Harmonisation with the European Union's GDPR would also be one-sided in terms of alignment requiring the Australian Government to do the uplifting to meet GDPR requirements. For example, all EU businesses are required to have a GDPR-compliant privacy policy. In the Australian context, not all governments or businesses are regulated by the same privacy legislation and to achieve harmonisation internationally would first require extensive work to align privacy legislation nationally between government and business.

In addition, it is also likely to require the Australian Government to legislate any proposed change and it would need to consider both reduced reporting timelines and corresponding increased penalties.

An alternative way forward would be to seek bilateral agreements based on mutual understanding of risk, standards and processes. This could in time lead perhaps to some wider multilateral agreements.

As noted above, the protection of individuals and businesses against non-state offenders is severely limited. While protection of government holdings is a priority, it would be useful if the Standards were framed in a way that could, in time, provide a greater measure of protection for non-government entities and individuals.

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?

A Principles based approach can allow both flexibility and subjectivity to creep in. However, history has shown that while a principled based approach can effectively support strategic direction or data security harmonisation arrangements, it often fails to achieve the successful implementation of the actual standards.

If assurances are to be made to the public and the desired uplift in government and small-med business enterprises is to be realistically achieved, minimum requirements must be stipulated. These must be 'non-negotiables' and not open to subjective interpretation or the community cannot rightfully expect (and trust) that a consistent approach to data security will be achieved.

The three core pillars of secure, accountable and controlled outlined in the discussion paper are useful but the key to the success of the Commonwealth in supporting an uplift in data security is the establishment of benchmark criteria to avoid predictable subjective or discretionary assessment of their meaning with subsequent inconsistency in application.

A cohesive and coordinated Government approach is essential to engender public trust however it should not be onerous.

Figure 3 (p 12) and Figure 4 (p 15) of the *National Data Security Action Plan* ('the plan') provides a good indication of how convoluted the current environment is in relation to state and commonwealth policy, strategy, legislation, initiatives, responsibility, guidance etc. It is subsequently very difficult for experts to be entirely across the rapidly evolving and changing policy landscape, much less laymen. There is an opportunity here if not for consolidation of requirements, a collaborative piece that draws these elements together in communications targeted to various audiences.

Understanding of data security risk in both the broader community and among the non-technical public service employees is relatively immature. Even technical IT experts may not be well informed in relation to the management of contemporary information/data issues. Information security has tended to focus on technology risk, threats and vulnerabilities, and associated system controls. An opportunity exists for more holistic approaches, ensuring Security strategy considers the relevance of governance (people, process, policy); business and privacy impacts; measuring, monitoring and reporting (audit and compliance); information lifecycle management; eDiscovery; business continuity and data recovery, etc.

It would assist the Tasmanian Government if the Australian Government were to provide materials that illustrate how new data security legislation will affect local governments and consumers - including specific guidance where high risk environments exist. This is likely to enable more effective engagement with those sectors and address their concerns in relation to data security legislation and compliance.

Additionally, the Tasmanian Government asks that the Australian Government provide guidance on the staged introduction of these protocols, noting that not all jurisdictions are adequately resourced.

Any data security guidance should include, align with and/or be informed by existing legislation that governs information including:

- Data integrity, emphasising quality (and defining this) over quantity. For example, personal information should be "accurate, complete, up-to-date and relevant" as per Personal Information Protection Act 2004 (Tas)[2]

[2] Data security

(1) A personal information custodian must take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure.

(2) A personal information custodian must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

(3) A personal information custodian, the records of which are subject to the Archives Act 1983 , must take the reasonable steps referred to in subclause (2) only with the approval of the State Archivist.

- Data protection, so that consumer data is protected, redundant and obsolete data removed and valuable data managed across the life-cycle including authorised, legal destruction or transfer to State archives under the Archives Act 1983 (Tas).

Not all government organisations have the capability or capacity to assess the security credentials of suppliers. An opportunity exists to establish a system which leverages work from across jurisdictions (the Commonwealth, state and territories, and New Zealand) and this should be able to be disseminated under the Inter-Government Agreement (IGA) for data sharing.

The EU, when rejecting Australia's data security standards , indicated that those of New Zealand were acceptable to it. This may provide a case study that can be applied to the Australian experience.

It is also recommended that the Australian Government establish and maintain a register of accredited multi-national, national, and state based organisations which could operate similar to - in line with the IRAP program and be expanded to encompass Government organisations to endorse suppliers for use by government entities. This would provide States and Territories with a central repository of accredited providers at their disposal. States and Territories could then build on this list by submitting prospective providers for accreditation acceptance to the central repository. There is also an opportunity to work with the consumer protection agencies to develop a certification scheme to assist non-ICT users to identify credible data security software and services.

The data minimisation principle, as applied to the EU's GDPR, aims to limit the collection, processing and storage of personal data and should also be considered a key policy position for this Action plan. It is important to ensure the risks of holding 'big data' for 'what if' moments don't outweigh the benefits. The less data held, the less to lose in the event of a data breach.

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?

1. What obligations are you most commonly subjected to from international jurisdictions?

A review and amendments of Australian legislation could deliver greater protections and legislated rights for consumers so as to manage:

- inconsistencies in legislation between jurisdictions, particularly where data are collected in one jurisdiction and stored in another
- data security standards required for international vendors
- data security where the collecting business or organisation falls under the threshold in the Commonwealth Privacy Act. Although pragmatic in intent, a size threshold is impractical when considering security uplift. Where constrained by size of resources and funds, rather than accepting lower levels of security and safety for consumers (or effectively blocking participation), government could direct small operators to central accredited support agencies, similar to the model of Accredited data sharing agencies under the ONDC and the Data Availability and Transparency Act 2022 Scheme (DATA Scheme). Such a scheme could be scaled according to the size of the entity.

Reducing barriers to the use of international vendors where issues of data sovereignty arise, and where local legislation may override Australian personal information security interests (eg US PATRIOT Act, The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region, etc.)

Page19 of the Action plan makes reference to protectionist governments establishing barriers to digital trade by preventing the free flow of data. If Australia is to promote free-flow of information

along the lines of free-trade agreements, clients could rightfully expect legislative recourse in the event of personal damage through loss or theft of their data. Legislative recourse, including any proportionate punitive measures, may improve decision-making with regard to the protections put in place by data custodians on behalf of their clients or customers. It may also instil greater trust in government, particularly should related support mechanisms be introduced.

Tasmania's international engagement is focused on trade and implementing Australia's international obligations in fields such as human rights, justice and security. We have a range of compliance and reporting obligations.

Variations in international approaches to data handling and security can impede trade activities for Tasmanian companies by lowering confidence, increasing red tape and raising risks of data compromise.

The Tasmanian Government urges the Australian Government to act circumspectly in proposing legislative change and consider other options in the first instance. Child protection, consumer rights and private international law should not be diminished by any agreements or legislative amendments arising from this Action Plan.

5. Does Australia need an explicit approach to data localisation?

To date, local storage requirements have been employed to protect sensitive information or information which may pose risks to the data owners, and national security threats if transferred overseas. At the Commonwealth level, Australia's legislation currently prohibits or restricts the storage, processing and transferring of certain data overseas.

These measures are in place to ensure that operating entities comply with reasonable Australian based operating laws, so they can be audited for financial compliance, and in the case of noncompliance, successfully litigated under Australian law.

Where cloud services store data and are not explicitly subject to localisation guidelines, data leakage to potentially undesirable locations can easily occur, often without the data owner's knowledge.

To relax this position and move to an environment where international data flows remain 'safe, secure, lawful and ethical and in line with Australia's values and interests' would require transparent safeguards to be firmly in place.

Australian consumers have specific legislation that protects their consumer rights throughout Australia. The same level of protections needs to be applied to consumer data. Australian consumers need to feel confident that their data is secure, and they have control over when and by whom that data is accessed. This should include a requirement for mandatory reporting and notification of all data breaches. However, any such requirement must be proportionate so that accidentally mis-addressing an email to one party is not treated the same way as deliberate or negligent release of multiple data items.

Like other consumer protection legislation, suppliers should be required to protect Australian consumers of their products and services by providing Australian-based victim support services. International suppliers might choose not to do this, but this information needs to be available so that informed choices can be made by Australian consumers.

More information is required on how any proposed approach will operate within the context of Australia's federal system. Overall, however, the Tasmanian Government supports the idea that Australian data should be stored locally.

4. STATE AND TERRITORY AND MUNICIPAL GOVERNMENT UPLIFT

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? If yes, why?

Harmonisation of security classification systems through the Commonwealth and jurisdictional protective security frameworks is a good place to start but will require significant effort and investment (both time and resources). Further clarity on how this may relate to sharing protected information (protected data) under the amended Security of Critical Infrastructure Act 2018 (SOCI Act) would be welcomed. Jurisdictions have limited understanding of how to share Commonwealth protected information within their own government information-sharing arrangements and the Commonwealth will need to review legislation and correct or align the terminology.

For intergovernmental data sharing, harmonised information classification and data handling methodologies is a pre-requisite. The information security management (ISM) should be used as guidance on control implementation for all Government systems and services that generate, carry or host data. Data localisation is an example of this.

There should be a consolidation of standards to establish a clear, consistent policy for government agencies to comply to. Currently, the Tasmanian Government and its suppliers are faced with a raft of security standards (such as the PSPF, ASD ISM, NIST and ISO27001) in addition to Tasmanian Government ones.

The Tasmanian Government is committed to the harmonisation of security classification systems and is informed by the Commonwealth PSPF in the co-design and development of the Tasmanian PSPF.

This will include the introduction of a uniform information classification model. The harmonisation of these areas across all levels of government would serve to improve data security, management, and handling.

So long as jurisdictions can assess any future framework based on assessed risk and sensitivity, a higher level of standardisation using the Australian Government PSPF should be achievable.

Consistent data security requirements may result in more uniform contractual arrangements, where appropriate. In the event that data security requirements are changed in the interests of national consistency, it is reasonable to expect that both industry and Government would require some transitional arrangements to be established to allow for existing contractual terms to come to an end and to allow for frameworks, procedures and relevant policies to be developed to address the requirements.

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?

It is expected this would be achieved through the Local Government Association of Tasmania and individual local governments, with support from the State Government (e.g. Local Government Division, Department of Premier and Cabinet).

Local government remain responsible for their own data security issues. Given the wide range of digital capabilities and security awareness in this space, its entirely understandable that some entities struggle to effectively manage their data security. Often this function is outsourced to a service provider.

Sharing the responsibility more broadly is likely to create confusion and therefore it should remain the responsibility of the authority or data owner. Ultimately, it's up to the data custodian if they outsource the delivery of services to ensure data security. Smaller local government entities may struggle to meet any harmonisation standard and will likely look to the State Government or service providers for support.

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?

There are many challenges observed and identified by the Tasmanian Government that industry faces resulting from inconsistent data security practices. The impact of these will be influenced by many factors including the industry's resources and scale of operations.

Key challenges outlined in the previous questions are summarised again and include:

- Complexity of information when working across multiple levels of government.
- Limited capacity and capability of business and community stakeholders to understand and address the different security classification systems and privacy legislation in Commonwealth, State and Territory and local government across Australia.
- Limited options to reduce risk caused by inability to comply with various requirements resulting in a culture that is accepting of being less compliant.
- Vendors doing business with government are faced with an inconsistent or incomplete set of security requirements.
- Uplifting data security and storage requirements with industry/suppliers is not likely to come without some additional cost for industry (which is ultimately passed on through fees to Government).

All levels of government including local government should be able to procure secure trusted products and services without additional burden of assessing supplier credentials. Suppliers should be able to demonstrate to a government organisation their capability to secure their provided services and/or product in a manner that minimises supply chain risk to government organisations.

For example, third party security in general is recognised as a high risk and concern for all levels of government. This applies to many areas of basic business, as well as those larger industries involved in supporting government(s') activities. Similar standards and protective measures should be applied to these third parties to improve data security practices and ensure the safeguard of government public facing outcomes.

This issue is currently only addressed via individual contractual arrangements with business/industry partners. There is no uniform approach nor legislative basis to compel businesses to meet the standards desired by government enterprises in undertaking their business activities. While this is considered a cost to running business, and likely to be passed onto customers, the consequences of not applying appropriate security measures can far outweigh the costs.

In terms of having different security classification systems and privacy legislation across the Commonwealth, State and Territory and local government jurisdictions, harmonisation would certainly assist in data exchange and service delivery. However, it needs to provide the client with mechanisms for 'informed consent' regarding the use of their data for the services they receive and not simply assume that as they gave it, it can be reused.

Additionally, informed consent should be based on information rather than coercion: "if you do not agree we cannot provide this service". Consumers should be able to review other government users of the information they provide. In a mature data security environment, this would be a point

at which consumers could select agencies or services they wished to have indirect access to their data. We recognise that Australia's data security and literacy environment is not yet at that level.

The Skills for Education and Employment (SEE) program funded by the Commonwealth Department of Education, Skills and Employment (DESE) was a recent example of the challenges faced by suppliers and training providers like the Tasmanian Department of Education and TasTAFE. DESE quite rightly wanted to ensure all training providers of this program were aware of data security. However, they went as far as requiring providers to be ISO27001 certified which was not achievable for most organisations and suppliers due to limited capacity and understanding of the accreditation process which meant the perceived cost of compliance would outweigh the benefits from the program. This example highlights the importance of uplifting data security skills and workforce capability of training providers and their suppliers.

5. CLARITY AND EMPOWERMENT FOR BUSINESS

The Tasmanian Government recognises this section of the discussion paper is specifically seeking a response from 'business', but offers the following observations considered relevant to questions 9 – 13.

9. What steps could your business take to better understand the value of the data they process and store? Do businesses have sufficient awareness of their data security obligations?

Based on observations by the Tasmanian Government, it is the view that businesses that have a data breach from a direct supplier should be able to have legal recourse against a supplier where they have clearly failed their obligations (via incompetence or neglect) to secure business data.

The Tasmanian Government, while not strictly speaking a 'business', does in part act as a business when dealing with its many clients and related state-based activities. The way to better understand the value of the data the Government owns and regularly uses is to link it to evidence-based decision making and deliverables. Without reliable and current data, the Government would need to either procure data commercially at a high cost or accept higher risks in government decision making.

Often, very basic data obtained in isolation is treated differently to clearly sensitive personal type data. While this may be appropriate in many cases, in an aggregated form even this basic data can become sensitive and desirable. Therefore, there should always be a minimum level of security onus placed on entities that deal with or accumulate data.

Based on observations and anecdotal evidence it appears that many businesses do not have sufficient awareness of their data security obligations. The solution to this issue seems always to be in improved education and awareness training for those involved with data management. Scaling this approach to meet the needs of small and medium enterprises is a challenge. The cost of requiring many micro/small businesses to complete a basic certificate in data security – similar to a food handling certification – outweighs the likely detriment to the business and its clients of a data breach. On the other hand, boutique or bespoke service providers' clients are likely to have a different level of detriment from data insecurity.

Improved consistency and transparency in the reporting of data breaches to drive improvement and maturity uplift is partially addressed under the remit of the Office of the Australian Information Commissioner (OAIC)'s Notifiable Data Breach (NDB) scheme. It would be worth expanding the scope of reporting to include data leaks that do not include personal data but may still require elevated protection. Lessons learned could be shared to support local risk and vulnerability identification and associated uplift.

Recognition is also warranted that cloud adoption does not always automatically assure an associated security benefit and is nuanced:

- A lack of internal expertise may mean entities assume security based on the use of a certified platform and may not always extend adequate scrutiny to the application or the software provider.
- Without escrow services for code and backup data, cloud may be higher risk than on-premise data stores.

10. How can the Australian Government further support your business to understand the value of data and uplift your data security posture?

Based on observations in relation to supporting businesses, it is the view of the Tasmanian Government that the Australian Government can further support businesses to understand the value of data and uplift data security posture by ensuring that sufficient implementation support is provided to critical infrastructure entities now captured under the SOCI Act who are required to comply with cyber security arrangements.

The setting of minimum levels of security on all entities that deal with or accumulate data might prove helpful.

Local business adoption and the impact of any such accreditation process is critically important to the Tasmanian Government. The Australian Government will need to provide clear support (or preferably fund), financial incentives to ensure local businesses are able to supply products and services to Government organisations. This should be risk based and be proportional to the services they are intending to supply to government organisations.

Other support strategies include developing and implementing an Awareness and Education campaign for the public on personal data security responsibility and risk, and planning for reliable and broadly available infrastructure to support the use of cloud and help agencies and users reap the benefits of flexible access to services.

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 recent history of malicious activity resulting from compromised supply chains, clearly suggests more focus and work is needed in this area. Generally, the need for appropriate supply chain data security is managed as part of individual contractual arrangements with vendors and agreed on a case-by-case basis. Reference is often made to ISO 27001, ISO 27040, ISM, NIST and SOC2 with regards to the managing and storage security of data. Ultimately, the onus falls on the customer to mitigate or accept any risks, and or to ensure an appropriate level of security.

Appropriate advice is available from authorities such as the ACSC (for example see Cyber Supply Chain Risk Management dated 6 October 2021), however, we understand even the ACSC struggles to get its messages to many medium and smaller businesses.

Improved data security awareness needs apply to all sized businesses. For example, there are now thousands of small Apps (IOS / Android) developers (potentially only a single person) who offer / sell "Apps" to end users which contain Personally Identifiable Information (PII) data that may not always be secured and comply with via best practices by the private sector.

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.

Based on observations by the Tasmanian Government of Tasmanian businesses of all sizes, there is a need for overarching guidance on data security, especially for small to medium sized businesses (SMEs).

In Tasmania, there are over 37,000 small businesses[3], with approximately 96% employing 1-2 Full Time Equivalent (FTE)s[4] who are likely to lack the knowledge and skills required when it comes to data security. When starting up a small business they will most likely not even consider data security needs. Government guidance and assistance through initiatives such as Business Tasmania and Digital Ready Program would go a long way to ensure they are compliant with relevant data legislation and their systems are secure.

The data security guidance for businesses should have a common minimum standard with a scaled escalation that reflects both the size of a company and the value of the data being stored. This will provide a basic level of protection for all clients but also recognises that industry resources and vulnerabilities vary, often by company size.

The setting of minimum levels of security and overarching guidance on all sized entities that deal with, or secure data is needed.

The approach to policy implementation should make clear the alignment with existing obligations for businesses. For example, changes to the Privacy Act implemented in 2018 require that Australian businesses with annual turnover in excess of $3 million must notify their customers and the Office of the Australian Information Commissioner within 30 days should they suspect or experience a serious data breach. The implication that breached personal data from companies with an annual turnover less than $3 million isn't considered just as serious, at least from the individual owner's perspective, seems inconsistent and in need of change.

It would be beneficial if the National Data Security Action Plan drew from the learnings gathered in the implementation of that change (e.g. in relation to achieving compliance levels and cohort engagement etc).

It is worth acknowledging the professional standards, development and certification model underpinning the Australian Computer Society (ACS)'s Trust Mark and Liability Insurance initiatives [5]developed for SME IT consultancies that aims to demonstrate their accountability and responsibility to the client. For example, the Liability Insurance policy specifically targets SMEs with a turnover of under $200K and the level insurance policy cover it determined by professional certification of the policy owner. The scope of the initiatives include: managed services, applications, cloud computing, cyber security, mobility and websites. It also helps SMEs achieve ISO 20000 requirements.

To lift the level of publicly managed regulation and monitoring for compliance for software vendors, support is needed to increase their commitment and capability to data security while retaining their ability to innovate and compete in the market.

Support is also needed for small business and small public agencies and organisations to understand the level of security and the level of risks associated with particular vendors and software applications.

[3] Business Tasmania (2020) Starting a Small Business in Tasmania. July 2020. https://www.business.tas.gov.au/__data/assets/pdf_file/0009/253485/Starting_a_Small_Business_in_Tasmania.pdf
[4] Tasmanian Small Business Council (TSBC). About - TSBC
[5] ACS Trust Mark ® | ACS; Liability Insurance | ACS

13. Are there any limiting factors that would prevent Australian industry and businesses from effectively implementing an enhanced data security regime?

One of the main factors observed by the Tasmanian Government that would prevent Australian industry and business from effectively implementing an enhanced data security regime is the lack of clear / uniform guidance and legislation across all state and territories and at the National level. Australian industry and business need to have confidence that the data security regime they put in place meets all their obligations in every state and territory they operate in.

In relation to broadly achieving 'clarity and empowerment for business' the approach to policy implementation should not include overly technical language as the level of digital literacy in the broader small business sector continues to be low.

It should recognise that achieving SME engagement on complex issues can be difficult (particularly if compliance is required) as they are time poor and feel burdened with 'red tape'. For the many smaller and medium businesses, it can also effectively become a cost issue when it can't be passed onto the consumer. Expecting small businesses to implement standards and processes at the level of large-scale businesses without appropriate support and guidance is not realistic.

Across jurisdictions there are also differing regulations in the registration of a business, perhaps as part of the business registration process there should be a form of compliance around managing data security.

Government, industry, and business are also limited by the lack of qualified cybersecurity trained staff.

In the blue tech sectors[6] such as engineering and advanced manufacturing, metals, electro-technology, renewable energy, building and construction, and agri-tech there is an increasing need for data security vocational education and training especially for mid-career para-professionals who are transitioning from apprentices/contractors to project managers of their own business, and who are also part of a supply chain.

6. EMPOWERING AND EDUCATING CITIZENS AND CONSUMERS

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?

'Empowering and educating citizens and consumers', will require a nuanced approach. Australia's general level of data literacy is low to poor and the Australian Digital Inclusion Index 2021[7] shows Tasmania as the most digitally disadvantaged state in Australia. [8] The sections where data literacy is higher are those that are most resilient to its loss or compromise[9]. For many citizens, the ability to

[6] TAFE Directors Australia (2020). Critical Role of Blue Tech and Digital Skills in Australia's Economic Recovery. August 2020. Critical-Role-of-Blue-Tech-and-Digital-Skills-in-Australias-Economic-Recovery-August-2020.pdf (tda.edu.au)
[7] ADII (2021) Australian Digital Inclusion Index 2021 https://www.digitalinclusionindex.org.au/
[8] TasCOSS. https://tascoss.org.au/joint-statement-on-digital-inclusion/
[9] Human Resource Director (HRD) (2022) Data literacy in HR: Why is Australia falling behind? | HRD Australia (hcamag.com), 6 Apr 2022

use digital devices and services has become a fundamental skill for navigating daily life in an increasingly digital world, and the COVID pandemic has exacerbated this issue.

Digital capability is significantly influenced by literacy, educational attainment, and income levels, as well as the availability of adequate telecommunications infrastructure. The success of efforts to educate citizens to know their rights, roles and responsibilities when it comes to the secure handling, storing and managing data would be improved by:

- ensuring a fully inclusive approach that consists of equity of access to the services and information (eg languages other than English and assistive technologies) such as an information campaign that provides information across the spectrum of data literacy outlining the following key points:
  - What is personal data;
  - How is it used;
  - How it can be protected by the individual, including how to react if those protections fail.
- using accessible language (ie simplified concepts),
- confirming that community perceptions of trust in the relevant institutions remain current,
- empowering trusted intermediaries to drive consumer education and promote the benefits; and
- providing parallel processes to ensure citizens who do not engage digitally are not disadvantaged, and to reassure and educate them in relation to how their data is protected.

More can always be done in this space, but it really comes down to the individual placing more value on their own data before they hand it over to government or private businesses.

While a range of information is available to business and consumers on-line, it often lacks consistency and is difficult to digest. For example, the ISM and PSPF are excellent resources, but overarching guidance about how to implement them and how to make them work together is absent.

Observations by Tasmanian Government agencies indicate that businesses and individuals often get lost within the mire of government public information sites. The business.gov.au, Australian Competition and Consumer Commission (ACCC) sites such as ScamWatch and the ACSC cyber.gov.au websites in addition state government business sites such as Business Tasmania are examples. There is a need for tighter integration and cohesion between the sites. The improved resourcing of reliable and authoritative centres such as ACSC would simplify where businesses, consumers and citizens could go for current information on data security.

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?

Government agencies are subject to public accountability in the event of a data breach. There is an expectation that these mechanisms will be strengthened as part of the overall legislative programme. However, accountability mechanisms should recognise honest administrative error and scales of impact.

Industry has taken a much more compliance approach to data breaches, focusing more on protecting commercial interests than on notifying and protecting consumer/client interests. This is an area that would benefit from improved mandated accountability mechanisms.

Public trust can be enhanced by providing easier access for consumers to review their personal data holdings, to withdraw or modify consent to its collection and use, and to remediate damage caused by data leaks.

The challenge is more to make government/industry aware of existing accountability and reporting obligations. Guidance on government and industry sectors obligations would be useful, particularly where it recognises the scale of resources and consequences for organisations of different sizes.

All entities (government organisations and business) should be held accountable, and responsible for the security and safety of the public data and personal information they acquire, store, and manage. At present, this often only occurs if Commonwealth data is involved, or in the case of a private business, if their annual turnover is in excess of $3 million[10].

The public have the right to expect that government (and industry) entities will act to protect their interests, work transparently, and implement the highest of standards. Where data breaches occur, incidents need to be owned, managed expertly and sensitively, and resolved quickly. An honest, timely and effective response to data insecurities will underline the integrity of those authorities.

Acknowledging the difficulties that this might place on small and medium business, this means suitable guidelines and accountability mechanisms need to be established at all levels to appropriately guide and report incidents and events.

Compliance monitoring and auditing of public sector organisations is a necessary addition to having "public sector organisations subject to a range of data security legislative and policy regimes that establish obligations to both classify and protect data sets". Having policy in place does not equate to consistent interpretation and/or application: transparency and independent regulation are required. Without these consumers may be misled in their level of expectation or assurance that standards are consistently met.

[10] Office of the Australian Information Commissioner (OAIC) https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities#OrgAndAgencyPrivacyActCovers