National Data Security Action Plan

Engineers Australia's submission

June 2022

ENGINEERS
AUSTRALIA

Contents

National Data Security Action Plan

Engineers Australia
11 National Circuit, Barton ACT 2600
Tel: +61 2 6270 6555
Email: policy@engineersaustralia.org.au

engineersaustralia.org.au

Introduction

Engineers are uniquely positioned to contribute to the development of the National Data Security Action Plan (NDSAP). Many of these matters have strong relevance to Engineers Australia members and stakeholders, including:

- Looking beyond policy and legislation to the concept of data and data integrity as a sovereign asset. A trusted Australia and an Australia that can deliver a national data security framework ("Action Plan") aligned with international standards and regulatory requirements of larger economic regions is in our best interests for maintaining Australia as a connected, accessible place to do business.
- Policy development that reflects a comparative analysis between US and EU data security frameworks to identify, acknowledge, and close legislative and policy gaps if required.
- Analysis of the impact on industry engagement at a national and local government level. Care must be taken that in defining a national data security action plan to satisfy the needs of the government; this does not unduly prejudice its implementation at an industry level.
- Skills and training requirements to evolve Australia's data security and integrity to the level where it protects consumers, local and national infrastructure/capability and maintains some degree of harmonisation with international standards. This will require a significant number of qualified personnel and relevant training programs.

Furthermore, Engineers Australia sees the issues arising in the discussion paper to be best captured rigorously through a disciplined Systems Engineering approach.

About Engineers Australia

Engineers Australia appreciates the opportunity to provide feedback to the National Data Security Action Plan. Engineers Australia is the peak body for the engineering profession in Australia. We are a professional association with over 110,000 individual members, constituted by Royal Charter to advance the science and practice of engineering for the benefit of the community. In regard to the NDSAP in particular, Engineers Australia can apply expertise in Cyber Security, Systems Engineering and Standards Development.

About this submission

This submission primarily responds to the 15 explicit questions posed in the discussion paper. However, we have also included some additional comments that more broadly arise from the discussion paper.

Contact

Engineers Australia welcomes the opportunity to engage further with the Department of Home Affairs. These are complex and contextual issues. Engineers Australia has significant expertise in our Learned Society Colleges and Technical Societies that can assist in addressing them. Please do not hesitate to reach out if you would like to discuss this further. You can contact us at policy@engineersaustralia.org.au.

Executive Summary

Challenge of complexity, particularly for SMEs and smaller government agencies

The complexity of laws in Australia and overseas and their interaction makes it difficult for businesses, especially small and medium enterprises, to understand their security risks and legal obligations. Of particular concern is protecting information that may relate to sensitive technical and commercial data, especially where the data is developed using third party software or other applications. This is exacerbated where that data may be held overseas and may be considered to have been exported under the various export control laws, and is potentially vulnerable to exploitation by foreign intelligence authorities or actors seeking to gain advantage from access to the data or breaching intellectual property rights.

Another significant challenge in data security and integrity appears when highly localised government entities with minimal resources are required to conform to standards and requirements that are misaligned with their organisational scale. Currently, each local government organisation is responsible for ensuring the uplift of data security via the creation of policies that are then implemented via such measures as:

- implementing security controls in their own IT systems, and
- placing requirements on suppliers to satisfy a baseline level of security.

Few businesses are fully aware of the security risks that their systems are vulnerable to. Businesses have to be critical about their bottom line and have sufficient commercial understanding of the data they process. Most need greater education on the cyber risks associated with different types of data stored within their systems or in systems shared with other entities.

However, it is also critical to ensure that no sector of the economy is regulated with punitive administrative overheads. There needs to be effective testing to ensure that the benefits significantly outweigh the costs of adopting such regimes. There will probably be scenarios where certain risks are accepted or managed in a low impact manner.

Mandatory reporting on data breaches would drive change towards appropriate data security regimes as businesses and other entities and their service providers uplift accordingly.

Data localisation

Data localisation should be at the heart of any sovereign Action Plan and is necessary to protect the information of individuals and businesses. Data localisation is increasingly becoming a national strategic and cyber warfare consideration. There are three main reasons why this is necessary:

1. Data localisation requirements enable governments to define the security standards of data storage and dissemination more clearly. This is fundamental to protecting government (particularly local government) and small business data integrity. This key guidance opportunity is fundamentally about establishing a consistent best practice.
2. Australia's economy depends highly on service-led industries. Data-localisation helps to entrench and protect those service industries to prevent them from being arbitrarily offshored.
3. Data localisation enables top-level response mechanisms to be more easily implemented in a large-scale cyber-attack.

Harmonisation

Data security policy could be better harmonised by creating a common data classification scheme to provide a common understanding of the security controls that are sufficient to protect that data for each type of data. While it is important to avoid a needlessly complex and prescriptive framework, creating policies based on a common underlying set of controls or guidance such as the Essential Eight, the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM) could be beneficial. Requirements for each jurisdiction would be mapped to the underlying guidance to identify commonalities. Ideally, there would be no differences in policies between jurisdictions. Note that this happens already with local government entities referencing the PSPF, albeit without thoroughly appreciating the policy requirements.

The use of conflicting or inconsistent standards increases the cost of doing business and requires time to identify the appropriate precedence of standards. The need for consistent, unambiguous language and the use of an authoritative glossary would help. There are examples of national cooperation, such as the national building code, which can be a model for developing a 'national data security code'. That code may start with, for example, the PSPF but progressively expanded and enhanced to be more relevant and applicable outside the Commonwealth Government context.

Balancing competing priorities

Australia will need a high-level principles-based framework to ensure the broadest potential for interoperability and compliance with international regulation. However, achieving efficiency of implementation will require disseminating well codified and defined laws that are sector-specific and aligned with the growth engines of the Australian economy. Identifying the key sectors most impacted by conformance with international standards and developing more narrowly defined, codified laws that can be straightforwardly enumerated (for example) in contracts would be beneficial.

The Action Plan will have to balance the dynamics between the need for innovation and competitive international market forces, promoting international and domestic competition whilst regulating and protecting Australian citizens' and businesses' data security interests. While broad advice is needed, only the minimum functionality should be specified, sufficient to satisfy each particular data security threat.

International "standards" dominate the compliance and data portability between Australia and our established and emerging trading partners. Portability and compliance are fundamentally important to Australia's economy and increase Australia's attractiveness as a place to live and work.

Variation in approaches creates hurdles to participation in the global market in the form of additional time and effort spent:

- understanding differences in obligations in different jurisdictions
- remediating systems to meet obligations
- completing independent assessment or certification to demonstrate satisfaction of obligations.

Australia should consider the adoption of international standards and frameworks. Aligning frameworks used in Australia with international frameworks would make it easier to demonstrate compliance. Where there appears to be no suitable international data security standard, Australia should develop and promulgate its own national standard through channels such as ISO and IEC. Mapping and aligning Australian legislative and policy measures against international frameworks from a trusted source is needed.

The Action Plan will need to be cognizant of protecting both ‘critical’ and ‘essential’ data. The discussion paper is silent on the fact that smaller entities managing services and data that enables the delivery of those 'essential' services increasingly rely on data to provide an essential service. This means that data is not getting the same protection focus as the designated ‘critical’ infrastructure.

The interface between national cyber security and the Government’s data security requirements for individuals and businesses is an important distinction. As a starting point, it is necessary to define the relationship of data security in the NDSAP context and where that sits within the overall national cyber security environment. The Action Plan needs to be clear about the boundaries between national data security and national defence data and how that will be managed.

Supply chain risk management

Supply chain risk is an emerging concept of higher significance for infrastructure service providers in 2022, following the lessons learned during the first 12 to 24 months of the current pandemic. Data security risks in the supply chain exist but are typically only being managed where mandated. Supply chain risks are difficult to quantify given the length of supply chains from component and product level through to system level, where vulnerabilities may exist without the knowledge of the business. While guidance is available on supply chain risk issues, the cost and time involved constrain small and medium enterprises from making those assessments. In addition, supply chains are almost always sector specific. This is an area where a national data security code would draw upon sector engagement (for example, utilities such as water and energy) to provide guidance on supply chain risks; noting that the Department of Industry, Science, Energy and Resources (DISER) is already in the process of undertaking supply chain risk mapping.

Reporting, assurance and public trust

Reporting of data security breaches is critical. This is important to maintain trust and integrity, but it is also a key data point that better equips government and industry to build a more precise characterisation of cyber security risk.

Public trust would also be engendered through a significant education and publicity program. Industry ownership would be required so that the community recognises and eventually demands effective accountability.

The concepts raised in the Discussion Paper would be enhanced by including greater discussion around assurance. What assurance is there that a (foreign) authority will continue to sustain an appropriate response to data security legislation and policy over the long run? If we accept that we cannot get appropriate assurances, how do we construct consensus and look for where we get the 'best' assurance?

Resources and Support

Organisations need to know where to find information before it can benefit them. More needs to be done to support awareness of risk assessments and gaps in data security. Online resources need to be easily accessible, particularly to organisations without any in-house cyber security experience, to provide guidance on what is available and what applies to them. The current ACSC website has a lot of information, but the documents are not easy to find.

Studies by the Department to canvas all sectors of Australian business and society are likely to raise awareness of the issues and risks while making best practice information more readily available. Industry associations should be a good initial source of what is most needed by companies. The information needs to be related to everyday activities and use case studies and specific examples to

provide more benefit than generalised scenarios. The goal should be for a progressive improvement rather than moving immediately to a high level of data security.

Overarching guidance should be available as a first step, with more detailed guidance based on sector, size, the complexity of IT environment and resources to address data protection.

Australia has inconsistent and conflicting data security terminology. The Australian Cyber Security Centre (ACSC) does a good job in this regard, and the Department of Home Affairs has a glossary on its main website, but there is an unmet need for a more mainstream and authoritative glossary of data security terminology and definitions.

A single centralised source of truth for data security policies and frameworks and consistent interpretation and mapping of international policies and frameworks would go a long way to answering these concerns.

Accreditation

A program of regular audit and accreditation would be beneficial, provided the positive cost-benefit trade-off for the business was demonstrated.

There is an opportunity for the government to define a more formal accreditation, and perhaps even a licensing scheme, for private sector actors to deliver services to the government, at least at the local level where it is most needed. This is an entirely reasonable way to scale data security capability in Australia as the needs of small businesses and local governments are not dissimilar.

Skills and Training

The government could further support businesses by defining training and education standards to underpin specific industries in close consultation with relevant industry bodies.
Government should consider refining immigration policies that give prioritised skilled visa access to operational expertise around international data security standards. From an industrial recruitment perspective, given that Australia has some unique and high-value niches, ensuring that the requirements and penalties scale with business size could be an attractive way to differentiate Australia as a data-driven economy.

Summary of Recommendations:

1. Take a principles-based approach that considers relevant international standards in established and emerging markets to maintain competitive advantage and compliance frameworks.

2. Provide clear overarching guidance on how sensitive content from a foreign entity should be managed.

3. In addition to the need for a principles-based framework to ensure interoperability and compliance with international regulation, the efficiency of implementation will require the dissemination of well codified and defined laws that are sector-specific and aligned with the growth-engines of the Australian economy.

4. Map international data protection and security frameworks with Australian standards, and where there is a gap, Australia should develop and promulgate a new standard.

5. Include guidance on the operation of export control laws, especially where technical data may be of dual military and commercial use.

6. Specify only the minimum functionality, sufficient to satisfy specific data security threats. Regulating or mandating specific measures needs to be carefully balanced against the potential to stifle the development of smaller and start-up businesses.

7. Ensure industry is aware of the principles and how they can be used through online resources, better practice guides, case studies and checklists.

8. Investigate providing a service for businesses of various sizes to discuss data security requirements and assist with validation of protection measures.

9. Data localisation should be at the heart of the Action Plan.

10. Provide clear, financially viable and prescriptive guidance on which data should be kept within Australia's legal jurisdiction.

11. Consider if there is merit in government agencies holding large quantities of personal data on Australians or data that is aggregated in repositories to be subject to localisation requirements.

12. Develop a common data classification scheme across all jurisdictions to create a shared understanding of the security controls that are sufficient to protect specific data.

13. Develop policies based on a common underlying set of controls and guidance, ideally with no differences in policies between jurisdictions.

14. Develop an authoritative glossary of data security terminology and definitions.

15. Consider centralising responsibility to ensure greater levels of data security expertise, allowing more robust and consistent standards, while at the same time allowing local governments to share knowledge on methods for implementing data security controls.

16. Consider creating an accreditation and licensing scheme for private sector actors to deliver services to the government.

17. Develop of a 'national data security code' applicable to all levels of government.

18. Provide education and information programs that raise national data security awareness for businesses and consider a cost-effective audit and accreditation program.

19. Develop a data sensitivity framework for private sector entities.

20. Further support businesses in understanding the value of data by providing guidance on the relevant legislation/regulation, the nature of threats, and a risk assessment process tailored to different levels of security knowledge and resourcing in specific industries.

21. Define the training and education standards to underpin specific industries in close consultation with relevant industry bodies.

22. Refine immigration policies to prioritise skilled visa access to operational expertise around international data security standards.

23. Provide public information on data security risks in supply chains to help businesses and service providers better identify and manage risks.

24. Ensure that legislative requirements are codified and portable; contractually able to be disseminated into the supply chain in a transparent and auditable way.

25. Provide both overarching guidance and more detailed information based on the organisation's size, the complexity of operations, and the sensitivity of data managed.

26. Consider a methodology to ensure the benefits of the data security regime outweigh the costs for businesses and industries.

27. Provide more information for consumers and citizens about their data security requirements. Work with consumer groups and industry associations to define what is needed. Dedicated websites will make it easier for people to find this information.

28. Enhance information around obligations in the event of data breaches and mandate greater transparency, including reporting against KPIs.

29. Either create a new role or strengthen the role of the Australian Information Commissioner and Privacy Commissioner to oversee data breach reporting and information sharing.

30. Define the relationship of data security in the NDSAP context, where it sits within the overall national cyber security environment, and the relationship between national data security and national defence data.

Response to the consultation questions

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

The complexity of laws in Australia and overseas and their interaction makes it difficult for businesses, especially small and medium enterprises, to understand the security risks and their legal obligations. Of particular concern is protecting information that may relate to sensitive technical and commercial data, especially where the data is developed using third party software or other applications. This is exacerbated where that data may be held overseas and may be considered to have been exported under the various export control laws, and is potentially vulnerable to exploitation by foreign intelligence authorities or actors seeking to gain advantage from access to the data or breaching intellectual property rights.

There is a need to balance the dynamics between the need for innovation, trials of new products, and competitive international market forces. Australia should maintain a balance between enhancing or promoting international and domestic competition whilst regulating and protecting Australian citizens' and businesses' data security interests.

For related classified interests, Australia enjoys its privileged status within the Five Eyes community and with our other international treaty partners. The unclassified application of data security principles will inform DHA's considerations. The emphasis here is on whole-of-economy rather than national security per se, which may be classified and accordingly be beyond the scope of this process.

International "standards" such as the EU General Data Protection Regulation (GDPR) and (from an enforcement perspective) the US Federal Trade Commission (FTC) Act dominate the compliance and data portability of international organisations between Australia and major economies (industry or government). As such, any Action Plan should carefully consider such standards. The Action Plan must inherently recognise that large parts of the Australian economy are already required to deliver against international standards to be competitive and compliant.

Cyber security readiness and threat management inherently involves validating and stress-testing systems that conform to a specific data protection framework. The demands of implementing systems compliant with, for example GDPR, create inherent implementation, resourcing, and capacity risk, particularly for local government and small businesses who are most vulnerable and where the aggregate economic damage is probably most significant. Therefore, it is critically important that a principles-based approach be established, while noting that this may not necessarily deliver conformance to countries such as the US, where enforcement is well codified in legislation, but data protection laws are highly fragmented and distributed at a federal and state level.

Given their relative maturity and global economic relevance, there will be a temptation to focus on EU/UK and US data protection frameworks. However, many emerging economies, vitally important to Australia, are starting to develop and codify basic consumer-focused data protection that did not exist even a decade ago. China is an obvious example of this, but there are others. Non-conformance to these emerging frameworks will be used to exert political and economic pressure, just as effectively as government-sanctioned cyber-attacks.

International information portability (and therefore compliance) is fundamentally important to an economy like Australia that will necessarily rely on immigration to meet our economic growth requirements over the next two decades. Efficient portability of key health (insurance eligibility), financial (benefits, pensions) and personal information (qualifications) will be an important part of facilitating this, ensuring it is efficient, has high integrity, and will increase Australia's attractiveness as a place to live and work.

Legislation in other countries may make it less likely or not possible for Australian organisations to store information overseas or use services that are only available overseas. For example, fears that the USA Patriot Act will allow the US Government to access any information stored in the US makes it unpalatable for some Australian organisations to use services that will result in information being stored in the US. Uplift of the data security and protection requirement may not resonate with multinational service providers. For example, clearance and background check requirements.

However, large service providers such as Amazon and Microsoft are being driven by Australia's data localisation requirements to set up local versions of services in Australia. This means that advanced IT cloud services are effectively just as readily available in Australia as in other parts of the world. This can mean the impact of internal barriers in preventing data security uplift is of less significance.

Australian infrastructure owners have contractors doing engineering and other design work that will want to send their development work offshore and currently lack guidance on how to best evaluate the security and safety of their data, or whether they do not send development work offshore at all. Given the demand for engineering design services in Australia relative to the number of Australian-based designers, not sending work offshore may be impractical.

Mishandling of data due to lack of guidance and clear direction on how sensitive content from a foreign entity also needs to be managed.

Other international barriers, such as bans on the export of specific technologies, do not significantly affect the availability of security tools and services in Australia and so also do not have a large effect on data security uplift.

Recommendation: Take a principles-based approach that considers relevant international standards in established and emerging markets to maintain competitive advantage and compliance frameworks.

Recommendation: Provide clear overarching guidance on how sensitive content from a foreign entity should be managed.

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)?

Australia should consider adopting international standards and frameworks, including for data protection. The European Union's General Data Protection Regulation (GDPR) is typical of developed standards. Those available regulations provide a good starting point for the NDSAP. Aligning frameworks used in Australia with international frameworks would make it easier to demonstrate compliance as the process would be identical or very similar to the process used in other jurisdictions.

GDPR Article 5.1-2 outlines a relatively straightforward principles-based approach to data protection, even if the full scope of the legislation is complex and challenging to implement. The attempt to harmonise data protection legislation at a supra-national level is commendable compared to the highly fragmented, complex and sector-specific approach. Nonetheless, a principles-based approach aligned with GDPR is necessary if Australian organisations are going to engage with the Euro-sphere effectively.

In the US context, there would be value in examining specific high-value industries where a general framework like GDPR is cumbersome, but where there exists relatively focused and defined legislation that facilitates specific data protection requirements. This is especially important for Australia given that economic growth will depend significantly on the export and delivery of services, specifically industries like healthcare and education.

Specific attributes could inform an Action Plan from legislation such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The advantage of looking at more narrowly construed data protection frameworks such as HIPAA are twofold:

- They tend to do a better job of codifying the basic compliance requirements in a way that is somewhat more straightforward to implement in contract and disseminate through the value chain of sector activity (to vendors and service providers). This is in stark contrast to a high-level principles-based approach, which tends to leave interpretation up to individual actors.
- A sector-specific data protection focus will demand specific regulatory agencies that are sufficiently informed and empowered to enforce legislation. Identifying and establishing these regulatory bodies will be an important part of any Action Plan.

Australia will need a high-level principles-based framework to ensure the broadest potential for interoperability and compliance with international regulation. However, achieving efficiency of implementation will require the dissemination of well codified and defined laws that are sector-specific and aligned with the growth engines of the Australian economy.

There are many frameworks and several of them are well known and already adopted by Australian businesses or applicable to them because of other jurisdictions they operate in, including:

- ISO 27k series (Information Security Management)
- SOC 2 (System and Organisation Controls 2)
- HIPAA (Health Insurance Portability and Accountability Act)
- GDPR (General Data Protection Regulation)
- NIST Frameworks – Government
- SOX – Finance
- PCI-DSS – Credit Card

Mapping of international data protection and security frameworks with Australian standards should be readily available from trusted sources. For example, mapping between the Information Security Manual (ISM), ISO 27001 and the National Institute of Standards and Technology (NIST) is not provided by the Australian Cyber Security Centre (ACSC) or the Digital Transformation Agency (DTA), or any other government agency. Organisations that need to interpret international standards to an Australian equivalent have to achieve that in an ad-hoc manner, which is not a consistent and reliable approach.

Where there appears to be no suitable international data security standard, Australia should promulgate its own national standard, with a view to subsequently having the national standard adopted by the appropriate international forum. There is no reason why Australia cannot lead aspects of data security internationally, with the potential to generate value for Australian businesses where Australia leads the engagement of emerging regional economies in the standards development process. An example of this is demonstrated by Engineers Australia's technical society, the Asset

Management Council, in the development and application of asset management policies and standards in, for example, Malaysia and Indonesia.

Recommendation: In addition to the need for a principles-based framework to ensure interoperability and compliance with international regulation, efficiency of implementation will require the dissemination of well codified and defined laws that are sector-specific and aligned with the growth-engines of the Australian economy.

Recommendation: Map international data protection and security frameworks with Australian standards, and where there is a gap, Australia should develop and promulgate a new standard.

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?

Identifying the key sectors that are most impacted by conformance with international standards and developing more narrowly defined, codified laws that can be straightforwardly enumerated (for example) in contracts would be beneficial.

Improved guidance on the operation of export control laws, especially where technical data may be of dual military and commercial use, would also be beneficial. For example, where Australian and overseas companies are collaborating on an engineering design and design data is stored in a cloud service that may be located overseas. The guidance should be delivered online and not behind paywalls. The principles should each be explicitly articulated, and the corresponding guidance and support should be directly linked under the relevant principle.

Engineers Australia cautions against too heavily regulating or mandating specific measures, which can stifle development and impose heavy dead-weight losses on smaller and start-up businesses. Only the minimum functionality should be specified, sufficient to satisfy each data security threat. Any formal objective compliance regime would be a complex and resource-intensive undertaking. It could impose high costs on Australian companies and ultimately could be counterproductive. In some cases, the only tractable approach is to adopt best practice and accept any residual risks.

The Australian Government currently describes security principles in the:

- Protective Security Policy Framework (PSPF) - 5 security principles
- Information Security Manual (ISM) - 24 principles arranged in 4 groups

While these are well-known to security practitioners that work in the Government and Defence industries, it is likely that the broader community is not aware of them. Therefore, the primary way in which the Government could assist with promoting a principles-based approach to data security is to communicate to industry that these principles exist and how they can be used. Case studies and examples are an excellent way to communicate how security principles can be implemented.

Online resources need to be readily available, particularly to organisations without any in-house cyber security experience, to provide guidance on what is available and what is applicable to them. This could be on the cyber.gov.au website or another location that is more likely to be found by a broad section of the community. Dated and version-controlled documents are best as they allow the reader to know if they refer to most recent advice. Guidance should preferably have "checklists" of items that need to be addressed, that make it clear what has to be done and the purpose of carrying out those actions.

An aspect of Government advice in the past was the development of publications like Better Practice Guides. Better practice guide type publications are particularly useful for smaller entities that do not

have the people or financial resources to figure out the basics for themselves. To require local government infrastructure owners to do that is a public policy inefficiency. Government outreach to support application of the guides will be required in the short term for the Government's investment in the guidance material to realise value.

The currently available guidance on the Australian Cyber Security Centre (ACSC) website is too generic to be helpful to many organisations. This could be compounded especially for small businesses because they may not be familiar with the defence websites or culture.

In addition, a public-facing consultancy service that can be contacted by businesses of various sizes to discuss data security requirements and assist with validation of protection measures would be beneficial. Engagement of an Infosec Registered Assessors Program (IRAP) certified assessor is expensive, complex, inconsistent and time-consuming.

Recommendation: Include guidance on the operation of export control laws, especially where technical data may be of dual military and commercial use.

Recommendation: Specify only the minimum functionality, sufficient to satisfy each data security threat. Regulating or mandating specific measures needs to be carefully balanced against the potential to stifle the development of smaller and start-up businesses.

Recommendation: Ensure that industry is aware of the principles and how they can be used, through online resources, better practice guides, case studies and checklists.

Recommendation: Investigate providing a service for businesses of various sizes to discuss data security requirements and assist with validation of protection measures.

4. How could Australian legislative and policy measures relating to data security be streamlined to better align with your obligations in international jurisdictions? Does variation in international approaches create hurdles to your effective participation in the global market?

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

Variation in international approaches creates hurdles to participation in the global market in the form of additional time and effort spent:

- understanding differences in obligations in different jurisdictions,
- remediating systems to meet obligations, and
- completing independent assessment or certification to demonstrate satisfaction of obligations.

Certain pieces of information may not be counted as having the same sensitivity across multiple countries. Contractual stipulations become key in this type of scenario. Personally Identifiable Information (PII) protection requirements are one of the common obligations that carry across jurisdictions.

GDPR (General Data Protection Regulation) and the CCPA (California Consumer Privacy Act) are the most common obligation from international jurisdictions that apply to Australian organisations

because of where customers are often located. Other US-centric frameworks, such as Service Organization Control 2 (SOC2), may apply to Australian organisations that wish to do business in the US.

Balancing these needs is a key challenge. On the one hand, European regulations require a very broad level of compliance with legislation that specifically defines the roles and responsibilities (and penalties for non-conformance), but there is relatively little sector specificity. The knowledge and understanding of how to implement GDPR from a systems, personnel and reporting standpoint requires very broad interpretation and a pan-organisation commitment to success.

The US, in contrast, generally implements data protection laws at a very localised and granular (sector) level (including reporting of non-compliance), but the Federal Trade Commission (FTC) as the notional top-level data protection enforcement agency still has very broad oversight and power to enforce (federal) principle-based data protection, typically driven from a consumer-focus concept of "deceptive practices". In implementation, it is possible to comply with a sector-specific or more localised data protection requirement but still not pass muster with the FTC.

This highlights the tension between a top-level enumeration of data protection "principles" and practical need for more localised, sector-specific needs. This is something that Australia needs to get right from the outset by prioritising what sectors most seriously need to align with international requirements. This, in turn, will necessitate considering what Australia's future economic mix looks like beyond our traditionally entrenched industries.

Australian policy could explicitly recognise and describe how satisfaction of obligations in international jurisdictions satisfies some or all Australian obligations. For example, if a product meets the US Government FedRAMP requirements, does this mean it is satisfactory for it only to meet a subset of the ISM controls?

As recommended above, mapping and alignment of Australian legislative and policy measures against international frameworks from a trusted source would be helpful. For example, protection measures outlined in The Australian Privacy Act and how that aligns with UK Data Protection Act and US Privacy Act.

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

With cloud-based services, data can be stored and managed anywhere in the world where local legislations and policies applies to data storage and handling unless explicitly agreed through service provider contracts. This can lead to poor security of Australian data in foreign countries that do not have a similar level of privacy requirements.

Data localisation should be at the heart of any sovereign Action Plan and is necessary to protect the information of residents/citizens and businesses. There are three main reasons why this is necessary:

- Data localisation requirements enable governments to define the security standards of data storage and dissemination much more clearly. This is fundamental to protecting government (particularly local government) and small business data integrity. This is a key guidance opportunity and is fundamentally about establishing a consistent best practice.
- Australia’s economy depends highly on service-led industries. Data-localisation helps to entrench and protect those service industries to prevent them from being arbitrarily offshored.
- Data localisation enables top-level response mechanisms to be more easily implemented in the event of a large-scale cyber-attack.

The requirements have to be clear, streamlined and economically viable to implement. There would be merit in Government organisations holding large quantities of personal data on Australians or data that is aggregated in repositories to be subject to localisation requirements.

Data localisation is increasingly becoming a national strategic and cyber warfare consideration. All ".au" domain data should be localised within Australia. That such data will inevitably also become localised into foreign domains is an unavoidable consequence of international online commerce, but this should be controlled as much as possible. Certainly, Australia should develop and promulgate Australia's policy on data localisation.

Smaller businesses and the general public cannot be expected to understand the risks of hosting data in other jurisdictions. Understanding these risks is potentially complicated because of the number of laws on this subject it would be a significant effort to understand and stay up to date with their implications for the privacy and security of the subjects of the information being held. Australian organisations need prescriptive guidance on which data should be kept within Australian's legal jurisdiction. This should be based on data sensitivity and protection requirements. Not all data need to be subject to onshore storage. Australia needs an explicit approach to data localisation that protects Australian data, but also provides the opportunity for new businesses to emerge that can be trusted partners in managing (foreign) data.

Recommendation: Data localisation should be at the heart of the Action Plan

Recommendation: Provide clear, financially viable and prescriptive guidance on which data should be kept within Australia's legal jurisdiction.

Recommendation: Consider if there is merit in government agencies holding large quantities of personal data on Australians or data that is aggregated in repositories to be subject to localisation requirements.

6. How can data security policy be better harmonised across all jurisdictions? What are the key differences between jurisdictions that would impact the ability to implement standardised policies/are there any areas of policy that could not be standardised? If yes, why?

Data security policy could be better harmonised across all jurisdictions by:

- Creating a common data classification scheme to provide, for each type of data, a common understanding of the security controls that are sufficient to protect that data.
- Creating policies based on a common underlying set of controls or guidance such as the PSPF or ISM. Requirements for each jurisdiction would be mapped to the underlying guidance to identify commonalities. Ideally, there would be no differences in policies between jurisdictions. Note that this happens already with local government entities referencing the PSPF, albeit without thoroughly appreciating the policy requirements contained therein.

Differences in privacy legislation between jurisdictions mean a set of security controls considered sufficient in one jurisdiction may be not considered sufficient in another jurisdiction. Therefore, standardised security policies would have to satisfy all jurisdictions, potentially leading to:

- Policies that are onerous and place too great a burden to be practically implemented, or
- Policies that have to satisfy contradictory legal requirements.

The DHA should harmonise Australia's data security policy with advice from the Attorney General's Department regarding the constitutional and legislative basis for such a mechanism.

There is a significant problem across Australia with inconsistent and conflicting data security terminology. The Australian Cyber Security Centre (ACSC) does a good job in this regard, but there is an un-met need for a more mainstream and authoritative glossary of data security terminology and definitions. A good starting point is the glossary provided by the United States "National Initiative for Cyber-Security Careers and Studies" whose website is at: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

Data security should not be confused with data integrity and protection in terms of relative policy importance. For example, GDPR requirements state that data security should use "appropriate technical and organisational measures". That "appropriate" measure is highly scalable and dependent on the use and needs of the data. To try and legislate that would be a waste of time and effort. There are certainly opportunities to provide guidance papers on "best practices" (ground-up security considerations, two-factor authentication, biometrics), but implementation should be competitively left to the private sector.

A centralised single source of truth for data security policies and frameworks, and consistent interpretation and mapping of international policies and frameworks, and standards would go a long way to answering these concerns.

Recommendation: Develop a common data classification scheme across all jurisdictions to create a common understanding of the sufficient security controls to protect specific data.

Recommendation: Develop policies based on a common underlying set of controls and/or guidance, ideally with no differences in policies between jurisdictions.

Recommendation: Develop an authoritative glossary of data security terminology and definitions.

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?

Australia's Constitution is silent on Local Government. Accordingly, Local Government from the Commonwealth perspective is whatever the Attorney General advises it to be, and possibly what the High Court deems it to be in due course. Responsibility for ensuring consistent and commensurate uplift of local government data security rests with the Minister for Home Affairs through their Cyber Security Policy and Coordination role.

The biggest challenges in data security and integrity appear when highly localised government entities, with minimal resources, are required to conform to standards and requirements that are misaligned with their organisational scale.

There is an opportunity for the government to define a more formal accreditation, and perhaps even a licensing scheme, for private sector actors to deliver services to government, at least at the local level where it is most needed. This is an entirely reasonable way to scale data security capability in Australia as the needs of small business and local government are not dissimilar.

Currently, each local government organisation is responsible for ensuring uplift of data security via the creation of policies that are then implemented via such measures as:

- implementing security controls in their own IT systems, and
- placing requirements on suppliers to satisfy a baseline level of security

However, responsibility should be moved to a centralised organisation or a state-based or federal-based organisation. This would ensure:

- the application of greater levels of data security expertise, allowing more robust standards that consider more advanced threats or complex risks, and
- consistent standards allowing local governments to collectively share knowledge on methods for implementing data security controls.

In the context of the Security of Critical Infrastructure Act, data security needs to go beyond 'critical' to 'essential'. The discussion paper is silent on the fact that smaller entities managing services and data that enables the delivery of those 'essential' services increasingly rely on data to provide an essential service. This means that they are not getting the same kind of protection focus that the designated critical infrastructure is getting. Current studies are looking at the non-critical systems and assets to understand how they may potentially impact critical infrastructure systems instead of considering the real impact on local communities with respect to the services on which they rely. The data security for non-critical infrastructure is required but is not subject to current policy advice at a Commonwealth level. There is justification for DHA to focus on systems of national significance, but that does not preclude DHA from developing policy to influence and facilitate other entities also managing their data security risks.

Recommendation: Consider centralising responsibility to ensure greater levels of data security expertise, allowing more robust and consistent standards, while at the same time, allowing local governments to collectively share knowledge on methods for implementing data security controls.

Recommendation: Consider creating an accreditation and/or licensing scheme for private sector actors to deliver services to government.

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?

The use of conflicting or inconsistent standards being used in procurement documents increases the cost of doing business and requires time to identify the appropriate precedence of standards. The need for consistent, unambiguous language and the use of an authoritative glossary would help. There are examples of national cooperation, such as the national building code, which can be a model for developing a 'national data security code'. That code may start with, for example the PSPF, but progressively expanded and enhanced to be more relevant and applicable outside the Commonwealth Government context.

Of course, the States are all sovereign and can independently do as they see fit, provided no national security risks arise. There is a real crisis in this regard, on the one hand a rigorous binding constraint is needed to make the issue tractable, however, the inherent creativity and competitive innovation should not be stifled by unnecessarily heavy-handed regulation.

Inconsistent data security practices between levels of Government result in the following challenges for organisations trying to implement security measures:

- understanding all requirements applicable to their operations

- complying with multiple sets of requirements
- unnecessarily restrict data sharing
- restrict collaborative work between agencies
- duplicated efforts and increased overhead on data handling.

Addressing these challenges requires additional time and resources that hamper an organisation's ability to conduct business or encourage behaviours where the appearance of security is implemented rather than actual security measures. Clearly, the latter scenario causes vulnerabilities in Australia's security posture, leading to adverse outcomes as described in the National Data Security Action Plan discussion paper.

Recommendation: Develop a 'national data security code' that is applicable to all levels of government.

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?

Few businesses are fully aware of the security risks that their systems are vulnerable to. Businesses have to be critical about their bottom line, or go broke, and accordingly have sufficient commercial understanding of the data they process. Most need greater education on the cyber risks associated with different types of data stored within their systems or in systems shared with other entities.

Government education and information programs help raise the national data security awareness for businesses. Some program of accreditation and regular audit would be beneficial, provided the positive cost-benefit trade-off for the business was demonstrated. Perhaps something like a 1 to 5-star ranking system could have competitive marketing benefits, and this could also better inform the National Data Security entity (DHA). Industry associations should own such a scheme with effective Commonwealth oversight.

At a national and international level, most businesses have an awareness of their obligations, but the question is that of implementation and compliance. Compliance can only be as successful as the clarity of codification of requirements, which comes back to general versus sector needs. An Australian Action Plan needs high-level principles-based codification to support frameworks that will be (ideally) largely interoperable with standards such as GDPR, but with sector-specific support to understand implementation.

A business could take the following steps to improve its understanding of the value of data it processes and stores.

- Map data flows and identify information assets and the protection mechanisms to protect those assets.
- Obtain advice from data security specialists who can advise on security vulnerabilities.
- Obtain advice from legal specialists who can advise on legislative risks from not complying with obligations to protect data.
- Obtain advice from people with experience in understanding and mitigating the business risks from failure to protect data such as loss of reputation or lost income due to impact on business processes.

Smaller businesses or those without the resources to seek expert advice are unlikely to be sufficiently aware of their data security obligations.

Development of a common framework to assess and measure data sensitivity based on the impact of compromised confidentiality, integrity and availability to the data owner would be beneficial. Currently PSPF provides the data sensitivity framework for Government data. A similar framework for private entities is needed.

Recommendation: Provide education and information programs that raise national data security awareness for businesses and consider a cost-effective audit and accreditation program.

Recommendation: Develop a data sensitivity framework for private sector entities.

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

The Australian Government could further support businesses to understand the value of data by providing guidance on:

- the nature of threats along with case studies that describe the costs of insufficient data security, and
- a risk assessment process that should be carried out to identify information assets and data protection risks and costs.

Ideally, this advice would be tailored for organisations:

- with different levels of security maturity
- with different levels of security knowledge and resourcing
- in different industries such as healthcare, infrastructure and energy.

Additionally, it would:

- describe legislation that places data protection obligations on an organisation
- comprehensively list security frameworks across Australia, and
- lists the more significant international regulations that place data security obligations on an organisation.

It would be beneficial to provide a mechanism for organisations to engage with the Australian Government representative/security consultant to help validate data protection measures for an organisation.

- More guidance for Boards and senior executives on data security issues for their businesses.
- Defining the training and education standards to underpin the industry, in close consultation with relevant industry bodies, will be important.
- Implementing effective immigration policies that give prioritised skilled visa access to operational expertise around international data security standards.
- For small and medium enterprises, grant funding and access to expertise, particularly as it relates to establishing an export opportunity.

Recommendation: Further support businesses to understand the value of data by providing guidance on the relevant legislation/regulation, the nature of threats, and a risk assessment process that is tailored to different levels of security knowledge and resourcing in specific industries

Recommendation: Define the training and education standards to underpin specific industries in close consultation with relevant industry bodies.

Recommendation: Refine immigration policies that give prioritised skilled visa access to operational expertise around international data security standards.

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?

Supply chain risk is an emerging concept of higher significance for infrastructure service providers in 2022 following the lessons learned during the first 12 to 24 months of the current pandemic. Data security risks in the supply chain exist but are typically only being managed where mandated. Therefore, data security risk in supply chains needs more public information from Government to help businesses and service providers better identify and manage their risks.
Supply chain risks are difficult to quantify given the length of supply chains from component and product level through to system level, where vulnerabilities may exist without the knowledge of the business. While guidance is available on supply chain risk issues, small and medium enterprises have difficulty in making those assessments due to the intricacies of supply chains and global sources of components, products and systems at all levels due to time and cost constraints.

Supply chains are almost always sector specific. This highlights the need to carefully identify the current and future growth sectors that most need support to consider data security needs and make sure that the legislative requirements are clearly codified and portable (contractually able to be disseminated into the supply chain in a clear and auditable way). This is an area where a national data security code would draw upon sector engagement (for example, utilities such as water, energy etc.) to provide guidance on supply chain risks; noting that DISER is already undertaking supply chain risk mapping.

Most security frameworks require that supply chain risks are considered to some extent. A business that is ISO27001 certified, for example, and does not have a large supply chain structure would be more confident that it considers risks than one with a large complex supply chain. For businesses in general, any organisation that is highly compliant or certified to a security framework should be considering supply chain risks in a manner that identifies risks and implements measures to address those risks.

The most well-known public information that assists or provides guidance on the identification of supply chain risks are as part of other frameworks, such as:

- The Information Security Manual from Australian Cyber Security Centre.
- Guidance for the risks of using cloud services from ACSC. ACSC currently provides guidance on Cyber Supply Chain Risk Management
- The Guide to Securing Personal information from the Office of the Australian Information Commissioner.
- Third party requirements in CPS234 from Australian Prudential Regulation Authority (APRA).

As with much data protection information, the main issue is that an organisation needs to know where to find this information before it can benefit them. Therefore, more needs to be done to support awareness of risk assessment to identify data protection mechanisms in place or any gap in data security.

Recommendation: Provide public information on data security risks in supply chains to help businesses and service providers to better identify and manage risks.

Recommendation: Ensure that legislative requirements are clearly codified and portable, that is contractually able to be disseminated into the supply chain in a clear and auditable way.

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.

Overarching guidance should be available as a first step. More detailed guidance needs to be based on a company's:

- size, including the complexity of IT environment and resources to address data protection
- industry, including types of data processed and stored
- risk tolerance.

Protection requirements may vary for a small company with local users compared to a large organisation exposed to global users.

The sizing parameters should relate to the perceived threat and may be based on total amount of data held and the typical rate at which that data was accessed or changed. Alternatively, indirect parameters such as turnover might be a useful threshold for the various level of guidance required.

This is a key challenge for GDPR as it is utterly daunting to small and medium enterprises, and the penalties for non-conformance have highly damaging thresholds. Ultimately, businesses that have a nexus with major market activity such as the US or EU already have to implement measures that deliver on data protection and security obligations. It should be the aspiration of an Australian Action Plan not to layer obligations and penalties that go above this.

From an industrial recruitment perspective, given that Australia has some unique and very high-value niches such as running clinical trials, early-stage pharmaceutical and medical device development, health services provision/concierge medicine that is increasingly international in scope, ensuring that the requirements and penalties scale with business size could be an attractive way to differentiate Australia as a data-driven economy.

Risk management would need to factor in such policy development as it would not take many case studies of data breach to affect Australia's sovereign reputation adversely.

Guidance on securing data should not just be based on size. A data security risk is a business risk that needs to be managed. The effort spent on mitigating the risk will consider the cost-benefit of doing so. All guidance should be based on the same set of principles. This will provide a consistent data protection message and allow an organisation to create a roadmap for managing their data protection as they change in size or modify their business processes.

Recommendation: Provide both overarching guidance and more detailed information based on the organisation's size, the complexity of operations, and the sensitivity of data managed.

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

Enhanced data security is always a good thing; however, it is critical to ensure that this sector of the economy is not over-regulated or hamstrung with punitive administrative overheads. There needs to be effective testing to ensure that the benefits significantly outweigh the costs of adopting such regimes. There will probably be scenarios where certain risks have to be accepted or managed in some low impact way. Mandatory reporting on data breaches will drive change towards appropriate data security regimes as businesses, other entities, and their services providers, uplift accordingly.

The limiting factors preventing Australian businesses from implementing enhanced data security are:

- Lack of qualified personnel. The rapid increase in the need for people trained in data protection has created a shortage of these people and an inability to fill roles. The Australian Government should consider increasing the number of people with cyber security training so that roles can be more easily filled.
- Lack of resources for tools and services. Security tools and services can be expensive, but there are also low cost or free tools available for some aspects of data security. Increasing harmonisation of security requirements across industries and jurisdictions will increase the body of knowledge available and may lead to greater adoption of more cost-effective solutions.
- Failure to appreciate the risks of poor data security. Organisations will only devote resources to improving data security if they see a need. A combination of greater awareness and increased compulsion from legislation or Government procurement policies will make the benefit of good data security more apparent.
- Standards of accreditation of people and firms.
- Country specific data privacy and sharing standards.
- Legislative restrictions.
- Intellectual Property protection.

Recommendation: Consider a methodology to ensure the benefits of the data security regime outweigh the costs for businesses and industries operating within it.

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?

Public information for consumers and citizens about their data security requirement and best practice needs to be increased. Information should be made available from the DHA website. Industry associations should be a good initial source of what is most needed by companies.

The broader community needs are more complex. The Department probably could run publicity programs and tap community groups to continuously monitor what additional information is likely to be effective in delivering enhanced data security. Studies by the Department to canvas all sectors of Australian business and society are likely to raise awareness of the issues and risks, while making best practice information more readily available. Information needs to be easily digested by general consumers and citizens.

Making consolidated information available online will make it more accessible. Dedicated websites will be easier to find and be more readable by consumers. The current ACSC website has a lot of information, but the documents are not easy to find and search function does a poor job of locating relevant information. Information needs to be provided with less jargon and more examples of what should be done to implement greater data security. The information needs to be related to everyday activities and use case studies and specific examples to provide more benefit than generalised scenarios. The goal should be for a progressive improvement rather than moving immediately to a high level of data security.

Recommendation: Provide more information for consumers and citizens about their data security requirements. Work with consumer groups and industry associations to define what is needed. Dedicated websites will make it easier for people to find this information.

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?

From a policy development perspective, what is important is reporting of data security breaches. This is not only critically important to maintain trust and integrity, but it is a key data point that better equips government and industry to build a clearer characterisation of cyber security risk. Enhanced information on data breaches is required to enhance accountability. While there will be a dip in confidence in the short term, routine reporting removes the sting while incentivising getting on with managing a key business risk.

The concept of enhanced accountability mechanisms for government agencies and industry in the event of data breaches is also non-trivial. If this were to be introduced the legislative requirement would be substantial and policing it would also be resource intensive. It seems inevitable that the independent sovereignty of the States could be a problem for the Commonwealth. The potential need to establish precedents through the High Court may be unavoidable. A compelling case would need to be established demonstrating the benefits over costs for such an accountability mechanism. Engineers Australia does not council against such a scheme but cautions that it may be a considerable undertaking.

Public trust will only come from the obligation of both government and the private sector to transparently report data breaches in a timely manner.

Public trust would be engendered through a significant education and publicity program. Industry ownership would be required so that the community recognised and eventually demanded an effective accountability mechanism for government agencies and industry in the event of data breaches.

Ideally, there should be no difference in accountability between government and the private sector. In this way there is an alignment of incentives (or disincentives) and is more likely to lead to well-developed standards of implementation and better consistency of understanding by service providers. Many local government agencies behave in such a transactional capacity, that it is hard to see the difference between government and industry at a practical level.

The Privacy Act 1988 allows for individual fines for breaches of the Act. This provides accountability for executives of organisations for the protection of personal information. Mechanisms such as

APRA's CPS234 also reinforces a culture of caring about data security. It is very visible in the US and Europe where you have large breaches. Affected parties have the right to sue, with significant adverse impacts for companies if they get it wrong. In Australia, there is not a requirement to report breaches. There is a need to either create a new role or strengthen the role of the Australian Information Commissioner and Privacy Commissioner and the Notifiable Data Breach Act to oversee data breach reporting and information sharing.

There is an assumption that commercial organisations will wish to avoid data security issues and its effect on their reputation. Organisations are aware that having a poor reputation can directly lead to loss of business and have adequate incentive to maintain a sufficient level of data security. Improving public trust in the government's ability to protect data will require greater measurement of security metrics and enforcement of penalties for not meeting goals. Implementing adequate data protection mechanisms should be included as departmental KPIs or measures of project success in government agencies. Sharing of threat information and mitigation efforts taken to address data breaches to help government agencies and industry to identify their vulnerabilities.
Reporting of attainment of data security goals and repercussions for not meeting goals would also provide assurance that governments are placing a high level of importance on protection data.

Recommendation: *Enhance information around obligations in the event of data breaches and mandate greater transparency, including reporting against KPIs.*

Recommendation: Either create a new role or strengthen the role of the Australian Information Commissioner and Privacy Commissioner to oversee data breach reporting and information sharing.

General Additional Comments

Complexity

The Discussion Paper and ostensibly the Action Plan comprehends massive complexity. This issue is illustrated in the discussion paper at Figures 3 & 4 in particular. There are: nine entities, intersecting with ten strategies or other instruments, through core or indirect relationships. Furthermore, those arrangements are enabled by at least four acts of Parliament, plus several Commissioners and other panels and manuals.

The discussion paper has done a good job outlining this complexity. Engineers Australia certainly agrees that data security is non-trivial. But given this complexity, the purpose of the Action Plan may be obscured, or is not immediately clear to data security experts or the casual reader. The naive observer might ask what is the Action Plan to do – who does what to whom and when? Certainly, the discussion paper makes it quite clear that the action plan applies to the whole of economy. Perhaps the strongest point that the discussion paper makes is that there is a clear well defined and measurable goal, which is: for Australia to be one of the world's top digital economies by 2030.

Furthermore, Engineers Australia believes there is a need to be clear about what the Action Plan does not include. For example, we understand that it does not include National Security, classified Communications Systems and the data security of the intelligence agencies. Nor does the NDSAP include Tactical, Operational or Strategic security data of the ADF or our allied partners. These exclusions are merely cited here to help sharpen the focus of just what it is that the action plan will do.

Cyber Security and the NDSAP

The NDSAP does comprehend an individual's personal data and that of industry and their associated Government regulatory and information sharing services. The Action Plan needs to focus on the explicit goal of providing Australian individuals and businesses with the trust and assurance required

to make Australia a top 10 digital economy by 2030. The interface between national cyber security and the Government's data security requirements for individuals and businesses will be a difficult balancing act. As a starting point, it is necessary to define the relationship of data security in the NDSAP context and where that sits within the overall national cyber security environment.

This issue is not just a matter of semantics! Is there a national data security versus national defence data interface and how will that be managed? Engineers Australia believes this issue is critical if the stated goal is to be achieved.

Recommendation: Define the relationship of data security in the NDSAP context, where it sits within the overall national cyber security environment, and the relationship between national data security and national defence data.

Assurance

The concepts raised in the Discussion Paper would be enhanced by including discussion around assurance with respect to data security. Points to consider:

- What assurance is there that a (foreign) jurisdiction will continue to sustain an appropriate response with respect to acceptable data security legislation and policy over the long run? However, we go about it, we need to be able to assure ourselves that we continue to maintain control over what we want to see happen with data, which will be a challenge with international agreements.
- If we do put data offshore to what we understand to be a high level or standard of data security laws and policies, how can Australians be confident that data and access to data will be managed appropriately or continue to be managed appropriately in another country?
- If we accept that we cannot get appropriate assurances, how then do we construct consensus to allow us to work with the variability of what is going to happen in the future? Should we be focusing on accepting that we cannot get assurance, and look for where do we get the 'best' assurance?
- A useful model for international consensus on data security policy is the Tax Information Exchange Arrangements (TIEA) between EU nations and Australia where there is agreement on how to share tax returns. Conversely, the EU has made adequacy decisions of data protection for personal data flows with New Zealand, Argentina, and Canada (partial) – but not for Australia.


ENGINEERS
AUSTRALIA