TELSTRA CORPORATION LIMITED

Submission to Dept of Home Affairs Discussion paper on the

National Data Security Action Plan

Public Submission

24 June 2022

Contents

Executive Summary

A digital economy built on a secure foundation is key to generating trust and confidence in the products and services that connect us all. Virtually every sector of the economy depends on the stable and secure functioning of the internet to deliver essential services to populations around the globe. Building this secure foundation is a shared responsibility for governments, the private sector and the community. We welcome the Government's initiative to develop an Action Plan to enhance and align data and cyber security across government, the private sector and the community.

Our submission makes four key recommendations for consideration. Firstly, we recommend a set of principles is developed alongside the three pillars outlined in the consultation. Principles describe *how* to get to the outcome articulated by the pillars and embody aspects such as proportionality, ease of understanding, avoiding overlapping/conflicting regulation and inclusion as examples.

Our second recommendation concerns regulation for data security. We propose the Action Plan ensures regulation for data security, privacy, critical infrastructure, etc. are harmonised, and that to the greatest extent possible, are constructed to avoid overlap. This should be done across layers of government (Federal, State/Territory and Local) as well.

Thirdly, we recommend secure-by-design features prominently in the Action Plan. Importantly, messaging for secure-by-design need to be crafted carefully to avoid creating the impression that security cannot be retrofitted. While it is always easier and cheaper to build security at the outset, in most cases it is still possible to add later.

Lastly, we provide our views on data sovereignty and localisation, recommending that where appropriate, Australian individuals, businesses and government should have the flexibility to specify where data is stored and processed. We consider guidance to be the most appropriate approach to informing Government and businesses on the risks and making decisions on data sovereignty and localisation.

Our submission concludes by answering the majority of the consultation questions.

01 Introduction

We welcome the opportunity to provide our views to the Department of Home Affair's Discussion Paper on developing a **National Data Security Action Plan**. We support the Government's initiative to develop an Action Plan that brings a consistent approach across all tiers of government to data security, aligned with international policies and practices. The threat landscape evolves at a rapid pace, and it is timely that the Government continues work to enable and empower businesses and members of the community to implement solid data security practices and mechanisms without unnecessary overhead, burden, or confusion.

The primary focus of the Action Plan should be facilitating an improved security posture through the development of principles, guidance, and frameworks rather than introducing new legislation or regulation. Our response to the discussion paper is intended to provide an overview of our thinking on the topics raised, and we would welcome the opportunity to discuss these themes in greater detail.

This Discussion Paper follows closely from the Department of Home Affair's July 2021 Discussion Paper on *Strengthening Australia's Cyber Security Regulations*, and much of our response to the July 2021 Discussion Paper is relevant to the questions posed in this new Discussion Paper, especially on topics such as efficient and effective regulation, and data sovereignty. We commend our August 2021 submission[1] to you.

02 What should the Action Plan cover?

We support the creation of a National Data Security Action Plan that identifies activities and a roadmap toward a clear and consistent approach to data security for public sector data, business data and personal information across all tiers of government. We recommend the Government establishes a set of principles to help identify and guide the development of tasks and activities in the Action Plan. Once principles are established, the Action Plan should address matters such as security by design, data sovereignty and the harmonisation and reduction of regulation to prevent overlapping obligations.

2.1. Principles and guidance

We recommend an early task for the Action Plan is to establish a set of principles to guide other tasks and activities in the Action Plan. While the Discussion Paper contains three core pillars[2] to underpin the Action Plan, we consider pillars are not the same as principles. The pillars describe the scope of the Action Plan by specifying matters to be addressed and what the outcome looks like; data is secure, custodians are accountable, and data is controlled both in transit and at rest. Principles, however, describe the fundamental elements on which components of the Action Plan will be based and annunciate *how* to get to the outcome.

As a case in point, the Digital Transformation Agency's Secure Cloud Strategy[3] contains some good examples within the seven key principles it articulates. Principles such as "*make risk-based decisions*

---

1 **Telstra submission** to Strengthening Australia's Cyber Security Regulation – Discussion Paper. 27 August 2021. https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/telstra.pdf

2 Discussion Paper, p.17.

3 Secure Cloud Strategy. Digital Transformation Agency, October 2021. https://www.dta.gov.au/our-projects/secure-cloud-strategy

when applying cloud security" and "*avoid customisation and use cloud services as they come*" guide users of the Secure Cloud Strategy in a way that helps them understand both the objective (outcome) as well as how to get to the end goal.

We consider principles underpinning the National Data Security Action Plan would include aspects such as: align security posture with the risk (proportionality); ensure security guidance is easy to understand and implement; avoid overlapping/conflicting regulation; inclusion to ensure all members of the community are brought on the journey; and so on. Principles such as these would sit alongside the pillars identified in the discussion paper to assist in addressing the matters we outline below, and we suggest the Department develop a set of principles to accompany the pillars.

2.2. Harmonise regulation and reduce overlap

We are concerned at the already burgeoning security regulation[4] and other regulation containing cyber security obligations.[5] In addition, there is a plethora of non-legislative requirements such as the Protective Security Policy Framework (PSPF), the Information Security Manual (ISM), and the Digital Transformation Agency's (DTA's) Secure Cloud Strategy that businesses and government must comply with, or at least have regard to. Adding to this collection will only exacerbate confusion and the burden on industry.

The Action Plan presents an opportunity to develop an overarching policy framework for security and protection of data and its use. Disharmony between regulatory frameworks is a barrier to investment and community confidence in the digital economy. Where it makes sense to, we recommend the Action Plan promotes a reduction in the amount of regulation to minimise burden on industry, alignment with international standards and policies to facilitate global trade, and compliance with existing laws. We also recommend there is scope to harmonise policies, such as data security classification across Australian jurisdictions.

As such, we strongly recommend a goal for the Action Plan is to harmonise, or better yet, reduce existing regulation while addressing overlap between Federal and state/territory legislative and non-legislative obligations.

As a starting point to reduction and harmonisation of existing regulation, we consider the existing Privacy Act, Australian Consumer Law (ACL) and Corporations Act regulatory frameworks have proven capable of effectively managing evolving risks, whether they be environmental, compliance or cyber risks. As we noted in our submission[6] to the July 2021 Discussion Paper on Strengthening Australia's Cyber Security Regulations, "…*we believe the existing, principles-based and technology neutral frameworks cited by the* [Cyber Security Regulations and Incentives] *Paper are fit for purpose and, while they do not provide for the direct application of specific cyber security standards, they do provide flexible and enforceable frameworks for addressing the issues of concern*." These frameworks should be the cornerstones against which other regulation is harmonised, or indeed reduced. We commend section 3 of our

4 Security of Critical Infrastructure (SoCI) Act, Privacy Act 1998, Corporations Act 2001, Telecommunications (Interception and Access) Act and Australian Consumer Law, to name a few.

5 **Strengthening Australia's Cyber Security Regulation – Discussion Paper**, 13 July 2021, p.12. "[Dept Home Affairs] *identified at least 51 Commonwealth, state and territory laws that create, or could create, some form of cyber security obligation for businesses*." https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-regulations-incentives

6 **Telstra submission** to Strengthening Australia's Cyber Security Regulation – Discussion Paper. 27 August 2021. https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/telstra.pdf

submission to the Discussion Paper on Strengthening Australia's Cyber Security Regulations to you in the development of the Action Plan.

2.3. Security-by-design

Data has significant strategic, economic, national security, and privacy implications, and security and privacy are fundamental to ensuring our economic success and way of life. Successful data security is essential to this.

We consider it important that the Action Plan contains activities to encourage "security-by-design" and "privacy-by-design". This is because attempting to add security or privacy to an existing product or service is almost always more difficult, and sometimes impossible, to introduce retrospectively.

One area where it can be particularly difficult to retrospectively harden the security of the system is in relation to data from Internet of Things (IoT) sensors and actuators (devices). IoT devices, as the title says, are connected to the Internet, and these devices are making their way into every industry including manufacturing, mining, transport, and health. Security on these devices can sometimes be quite low, and the only ways to secure them is to either put a shield (such as a firewall) around them, or replace the device entirely, because retrofitting the actual device itself is not possible.

2.4. Data sovereignty and localisation

We are keen to ensure that where appropriate, Australian individuals, businesses and government can specify where data is stored and processed. We appreciate there are onshoring requirements for certain types of data, such as data for national security purposes, health, etc. These specific sovereignty and localisation requirements can be effectively met contractually.

Outside of those data types, we consider guidance to be the most appropriate approach to informing Government and businesses on making decisions on data sovereignty and localisation. Guidance, rather than regulation, will ensure data custodians are informed of the risks while retaining the flexibility to make decisions best suited to the requirements of all the jurisdictions they operate in.

In terms of developing guidance for data custodians, we propose a more nuanced approach than the simplistic position of "*onshore storage = secure; offshore storage = less-secure*" is adopted. For example, a multi-national company operating in many jurisdictions may find storing data in another 5-eyes country may be more cost effective or delivers better customer service than onshore storage in Australia. Data storage facilities will be available in these countries that comply with a range of security levels, and sovereign risk will be low, such that data could be stored offshore in these countries while still meeting customer expectations or requirements in relation to privacy and security. Guidelines that help data custodians understand the appropriate level of security and the possible risks in international jurisdictions would be an appropriate solution to managing data sovereignty, while permitting flexibility.

03 Definitions and international alignment

There is a plethora of terms used by government and industry to explain data security. Providing clarity and consistency to the relevant definitions of data security, data handling and storage processes will enhance regulatory certainty across the economy and provide greater confidence for consumers. We recognise the benefits of cross-border data flows, particularly in a rapidly evolving global digital economy, where it is balanced with an appropriate level of protection, such that data remains secure.

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

While we don't identify any specific international barriers to data security uplift in Australia, there are nevertheless several factors that should be considered from international jurisdictions where learnings for Australia can be made.

Recently we have seen a more restrictive approach to data localisation and the free flow of data in several international jurisdictions, including Hong Kong, India and China. This makes it difficult for multi-national commercial agreements, as it can impact the sovereignty of Australian data being hosted or stored in an international jurisdiction and/or limit what data can be hosted or stored in Australia.

When considering a data security uplift in Australia, there is a fine balance between providing suitable protection of Australian data versus overly onerous data security requirements and sovereignty laws. We suggest that Australia looks to harmonise data security standards with likeminded nations, while as much as possible allowing for the unimpeded flow of data, where and when it is appropriate to do so.

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)?

Australian Government guidance on data security standards/cyber security should aim, where appropriate and where it is not overly onerous to do so, to align with international frameworks of likeminded nations. We consider it would be better to have a set of cyber security baseline requirements based on appropriate elements of international standards. For example, the draft rules for cyber security hazards developed as part of Risk Management Program under the *Security of Critical Infrastructure Act 2018 (Cth)*.

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?

Beyond the guidance we have outlined in sections 2.1 and 2.3 related to principles to achieve a stronger posture on data security, we have not identified any additional guidance or support that we specifically require from Government. We defer to others to articulate needs for their situation.

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?

We propose domestic laws are streamlined around a single set of principles and the pillars described in the discussion paper. See section 2.1 for further detail on principles.

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

Australian individuals, businesses and government should have the flexibility to address data sovereignty issues contractually, rather than through legislated obligations, and we discuss this in section 2.4.

04 Alignment across tiers of Government

Harmonisation across state, territory and municipal governments will be beneficial from a data security and classification perspective. Creating a common set of security definitions will allow all levels of government to work towards providing a seamless level of protection when handling sensitive and personal information.

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?

A single approach to data classification across all jurisdictions would be immensely helpful to business. The status of bespoke security classifications for each state/territory leads to complexity, additional challenges for engaging at Australia-wide level, and the potential for a citizen experience to become disparate depending on the jurisdiction they reside in or are engaging with. A single approach to classification could provide simplification, aid in data sharing across jurisdictions (where appropriate) and contribute to increased trust.

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?

No response.

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?

While we consider this is not a challenge for us, we note for the Department's record that we consider Federal laws and obligations apply to any/all telecommunication data, and that state/territory laws and obligations in relation to data security requirements only apply by contractual agreement. For completeness, we would be strongly opposed to state/territory laws applying to telecommunications data, as this risks fragmentation of obligations resulting in complexity and potentially in confusion for consumers.

05 Empowering business

Businesses are increasingly generating data, including personal information of consumers and data used for business operation. However small to medium sized entities are often less equipped to securely manage data. Private sector standards also vary between organisations which can lead to unnecessary confusion in how data is held. It is imperative that industry across whole of economy is committed to raising awareness and contributing to a stronger data security posture. Guidance provided by

government should account for various factors relevant to an entity's data security practices, beyond the size of the business to ensure a wholistic layer of protection is applied to data. We also consider that businesses have an inherent responsibility to assess their practices and processes for vulnerabilities and work towards uplifting their own data security postures.

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?

Telstra has a mature security framework and considers all hazards in our resilience and risk planning in relation to data we store and process, including where data is stored or processed by contractors. As such, we have not identified any additional steps we could take to understand the value of our data, or the risks associated with its storage or processing. We defer to others to articulate needs for their situation.

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

No response.

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?

Telstra's security framework carefully considers supply chains, and we have mechanisms in place to assess data security risks in these supply chains. We have a dedicated Partner Assessment team within the office of the Chief Information Security Officer, with a well-established set of cyber-security controls appropriate to a wide range of partners across a wide range of data risk profiles. The Partner Assessment team conduct reviews on all our partners who hold or process data about Telstra, its network and customers. This includes supply-chain partners. The Partner Assessment team and the cyber-security controls against which we assess our partners align to the ACSC's Cyber Supply Chain Risk Management.[7]

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.

While the size of the business potentially has some bearing on the risk of inadequately secured data, both in the sense of the size of the target and the scale of what could go wrong, there are many other factors that could contribute to the impact of a data breach. These factors include:

- Sensitivity and volume of data (together, "Aggregate Data Sensitivity"), noting that a small data processing house (i.e., a small business) could potentially process large volumes of data and/or data that is highly sensitive;
- Whether the data is shared and with whom (control of data); and
- Role played by the entity (i.e., generator, carrier, platform, data centre, data user).

We consider any guidance developed to assist businesses in securing data should be designed around a risk profile based on these factors, rather than on the size of the business.

7 Cyber Supply Chain Risk Management, October 2021. https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Cyber%20Supply%20Chain%20Risk%20Management%20%28October%202021%29.pdf

06 Empowerment and education of citizens

While there are many benefits to the increased digitisation of service delivery and the broader economy, correspondingly, consumers may be less aware of where their data is held and how it is used. Consumers need to be continually empowered and educated to remain vigilant and aware of the best practice habits that can improve their cyber hygiene. Businesses and government have responsibilities to uphold the privacy and security of consumer's personal information, which can be assisted by individuals following the advice offered through the existing guidance offered by various government agencies. Any further accountability mechanisms considered for industry in response to data breaches, should ensure that it does not create further undue regulatory burden.

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?

We consider there to be sufficient information and resources available to inform citizens of the importance of good data security, and a great deal of effort appears to have gone into making the information easy to understand and accessible. Programs such as Be Safe Online from eSafety Commissioner and resources[8] from the Australian Cyber Security Centre appear at the top of search engine results for phrases such as "cyber security" and "cyber safety". These resources teach people about the importance of securing data and personal information.

And yet, community attitudes can be slow to change. A Google / Harris Poll survey[9] of 3,419 citizens in the USA shows many remain blasé about data security, using common, easy-to-guess passwords. Education through school and other community programs (e.g., seniors) linked to the already available resources mentioned, is likely to be the most effective way of raising awareness and encouraging citizens to adopt safer online practices.

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?

With regards to the telecommunications sector, we consider the current regime of notification and reporting obligations under legislation such as the *Privacy Act 1988 (Cth)* and Telecommunications Sector Security Reforms (TSSR), and the incoming critical infrastructure reforms contain sufficient obligations for responding to, and reporting data breaches in the telecommunications industry.

8 For example, https://www.cyber.gov.au/acsc/view-all-content/advice/passwords-pins-and-passphrases and https://www.cyber.gov.au/learn/passphrases

9 https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf