2023 – 2030 CYBER SECURITY STRATEGY LEGISLATIVE REFORMS CONSULTATON PAPER

Telstra Response

1 March 2024

Introduction

Telstra welcomes the opportunity to make a submission in response to the Department of Home Affairs 2023-2030 Cyber Security Strategy Legislative Reform Consultation Paper (the **Paper**).

We support the Government's objective of uplifting and sustaining cyber resilience and security across the Australian economy. We acknowledge the important role that industry-government consultation has in shaping and designing reforms to address gaps in the existing framework and to strengthen our cyber shields to better protect individuals and businesses.

Cyber security is at the forefront of Telstra's strategy. It underpins the security of our critical infrastructure and the services we provide to Australian consumers and businesses. We are a strong supporter of industry and Government collaboration and threat sharing and we have a long history of working alongside the Australian Government on both operation security and cyber policy issues.

We encourage the Government to be bold in its approach to uplifting cyber security and national resilience. However, we caution against the introduction of new regulation in what is already a complex legislative environment unless it is clear, targeted and effective.

Our submission provides in principle support for Measures 1, 2, 4, 7 and 9.

We suggest that the Government provides additional clarity to industry about restricting the ASD and National Cyber Coordinator from sharing cyber incident information with regulators and law enforcement under the proposed limited use obligation (Measure 3). We also query the rationale and practical impact of introducing new 'last resort' consequence management powers (Measure 6), and review and remedy powers (Measure 8), under the *Security of Critical Infrastructure Act 2018 (*Cth*)* (**SoCI Act)**.

Finally, we do not support expanding the scope of the SoCI Act to capture secondary storage systems and business critical information (Measure 5). The protection of personal data is most appropriately addressed in the *Privacy Act 1988* (Cth) (**Privacy Act**), and the Risk Management Program obligations under the SoCI Act already require critical infrastructure entities to consider secondary data storage systems and business critical information to the extent that they could have a relevant impact on the entity's critical infrastructure.

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

Telstra supports the intention to introduce a mandatory secure by design standard for Internet of Things devices. We consider it best practice to follow established international standards, many of which defer to the ESTI EN 303 645. The first three principles of the ETSI EN 303 645 (no universal default passwords, implementing a method to manage reports of vulnerabilities and keeping software updated) are important guardrails in improving consumer safety and experience with their devices. We believe these represent an appropriate minimum standard.

We suggest a broad lens is applied to the consumer devices that will be captured by the mandatory standard and that exceptions should be considered for certain devices, balanced against existing regulation and levels of risk. Creating minimum standards that run along the spectrum of the supply chain would be beneficial to encourage secure by design principles from the build and design stage..

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

Ransomware attacks have seen exponential growth in recent years and some businesses may believe they have little recourse but to pay ransoms. Telstra's view is that prohibiting the payment of ransoms would provide clarity to victims of cyber-crime and insurers about the options available to them following a ransomware attack.

The Government is proposing two mandatory ransomware reporting obligations aimed at enhancing the national threat picture; where an entity is impacted by a ransomware attack and if payment is made. For

entities captured by the SoCI Act, the ransomware reporting requirements could be incorporated into existing mandatory cyber incident reporting obligations. However, the Government already has data about cyber incidents impacting this cohort, so the ransomware reporting obligations would also need to apply beyond SoCI Act entities if improved visibility of the national threat landscape is to be achieved. For consistency, we recommend maintaining timeframes for reporting that align with existing reporting obligations, such as those in the SoCI Act.

Enforcing a no-fault and no-liability protection principle will encourage entities to feel more confident in reporting ransomware or cyber extortion attacks. We also suggest that a tiered civil penalty provision for non-compliance with the mandatory reporting scheme would strike the right balance. We urge the government to consider how penalty schemes would operate where an entity has multiple reporting obligations.

The information outlined in the Paper to be included in a ransomware report would be practical and valuable to informing the national threat picture. Additionally, the reasoning behind why an entity has chosen to make the payment will create useful insights. There may also be exceptional situations to account for the payment of ransoms, where there is a significant threat to life, national or economic security - useful information for the Government to gather. Sharing the insights that are received in anonymised or aggregated manner quarterly with industry will help businesses to prioritise their cyber defences. If the report was able to collate information that could establish patterns or draw inferences across specific industries or sectors, sharing this through established Trusted Information Sharing Networks (TISNs) would be useful.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

Telstra maintains an established, proactive and trusted two-way relationship with the Australian Cyber Security Centre (**ACSC**). We believe that a limited use obligation could present a good opportunity for the ACSC to build trust and engage with entities that experience a cyber incident and do not currently have strong working relationships with the ACSC.

To provide certainty to entities that share information with the ASD and National Cyber Coordinator, we support limiting the ASD's and National Cyber Coordinator's sharing of that information to a defined set of prescribed cyber security purposes. We recommend being clear that information an entity shares with the ASD and Cyber Coordinator in relation to a cyber incident will not be shared with a regulator and will only be shared with law enforcement for the limited purpose of identifying and disrupting the threat actor. This is not clear from the prescribed cyber security purposes listed in the Paper.

While regulators have an important role during and after a cyber incident, they already have regulatory mechanisms in place for obtaining information about an incident (for example, through direct engagement with the entity, mandatory notifications, directions and information gathering powers). Similarly, law enforcement has coercive powers to obtain information from an entity.

It is important to also consider the other reasons why entities may not report incidents to the ACSC, that are not addressed by introducing a limited use obligation. There may be a perception that the ACSC may not be able to offer meaningful assistance due to resource constraints, may not understand the technical complexities of the network involved in the incident or leave the impacted entity out of key decision-making processes that impact their business. The ACSC should consider the role that they are capable of undertaking in such events and socialise this with entities to build trust between industry and Government and manage expectations as to how the ACSC would act in specific incident scenarios.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

A model similar to the US Cyber Safety Review Board (**CSRB**) would be an effective post-incident review and consequence model. The scope of the CSRB extends to both Government and industry systems,

threat activity, vulnerabilities, mitigation activities and agencies responses. This could be housed within the Office of Cybersecurity within the Department of Home Affairs.

Telstra submits that the Cyber Incident Review Board (**CIRB**) should be convened with both Government members and industry representatives and chaired by the National Cyber Coordinator. We align with the option suggested in the Paper to have a model that includes standing CIRB members and a selected pool of members on standby, who could be appointed to participate in the review depending on the type of impacted entity, nature and extent of the incident being reviewed. Members should include technical experts that can understand the mechanics of how an incident may have occurred, including those in academia able to provide perspectives on emerging tech that could prevent such incidents occurring in future. There should be representatives from key critical infrastructure sectors and established TISN groups, where members could be required to sign a non-disclosure agreement to cover the information shared by private sector entities. As part of the terms of reference, we suggest that a process for declaring a conflict of interest is established, consistent with existing legislation or similar bodies.

The purpose and scope of the CIRB should be set out with terms of reference or charter, equivalent to the US model, requiring reviews that are conducted on an independent and impartial basis. Consideration should also be given to the scope and impact of an incident, before the CIRB is engaged, and these parameters should be clear, with its role intended to only be advisory in nature and operation. This ensures that any review of lessons learnt are applied through a 'no fault' lens.

We understand that the scale and occurrence of cyber incidents is increasing and support having a threshold for initiating a CIRB review, particularly considering the impact of the incident on national security, economy and the broader public. We also suggest that the threshold for engagement by the CIRN allows for the possibility that events can occur across protracted time periods and investigation in circumstances where innovative methods have been used in the incident.

The viability of conducting a review will also depend heavily on the availability of relevant information and intelligence that can be gathered relating to the incident. We suggest that the power to initiate the review should sit with National Cyber Security Coordinator in consultation with the CIRB. We consider that the CIRB should initially be established with voluntary powers to request information. This assists in building up the reputation of the CIRB as an advisory body, capable of providing information and recommendations to the public to help uplift cybersecurity across Australia. Following a period of operation, the need to provide limited information gathering powers could be evaluated against the effectiveness of the board's existence.

Measure 5: Protecting critical infrastructure – Data storage systems and business critical information

Like many entities, Telstra complies with several data protection laws, including the Privacy Act, *Telecommunications Act 1997* (Cth) and *Telecommunications (Interception and Access) Act 1979* (Cth). So, we welcome the Government's commitment to limiting regulatory duplication. We view harmonisation of existing data protection regulations and reducing complexity in the storage and protection of data as pivotal to being able to successfully secure customer data.

The Government proposes to expand the assets captured by the SoCI Act to include any secondary data storage system operated by a critical infrastructure entity, where that secondary system holds business critical information that could have a relevant impact on the entity's critical infrastructure. While we recognise the importance of securing data storage systems and information, we do not support this proposed expansion of the assets captured as critical infrastructure under the SoCI Act.

It is not clear how the existing SoCI Act obligations and powers would apply to the secondary storage systems and business critical information. The objective of the SoCI Act is to uplift the security of Australia's critical infrastructure. It would be regulatory overreach and a burden on industry to extend all obligations under the SoCI Act (including the positive security obligations and Government powers) to secondary data storage systems holding business critical data. Such systems and information are not critical infrastructure and should only be captured by the SoCI Act to the extent a critical infrastructure

entity has assessed that the system or information could have a relevant impact on their critical infrastructure.

Most entities (including critical infrastructure entities) have obligations under the Privacy Act to protect and secure personal information. Many entities, such as Telstra, are also subject to additional data protection regulations. It will be confusing and duplicative to expand the SOCI Act to now also capture personal information, particularly as the SoCI Act does not apply to many entities in the broader economy holding vast amounts of personal information.

Part 2A of the SoCI Act requires critical infrastructure entities to implement, maintain and report on a Risk Management Program that identifies material risks that could have a relevant impact on their critical infrastructure and, as far as it is reasonably practicable to do so, to mitigate that impact. This means that critical infrastructure entities must already consider data storage systems and business critical information that could have a relevant impact on their critical infrastructure as part of their Risk Management Program obligations. Any lack of consistency in the application of these risk management obligations is most effectively addressed by updated guidance materials.

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers

Telstra understands that there may be a gap in the public's perception of the Government's role in responding after a significant incident. However, we query the effectiveness of new last resort consequence management powers.

As a critical infrastructure provider, our risk management and incident response planning outline the processes and procedures we follow if an incident occurs. We also maintain a strong working relationship with various government agencies, sharing information as necessary, built into these incident response plans.

Telstra remains committed to improving the national response to incidents by working with government through the established processes of the National Cyber Coordinator, the Australian Government Crisis Management Framework and the National Emergency Management Authority. We also consider there is great value in participating in cross-sector industry exercises, orchestrated by Government to foresee any gaps in our incident handling processes.

We suggest clarifying the rationale for the proposed new consequence management powers given these established processes and the proposed changes to the SoCI Act and the Notifiable Data Breaches Scheme to facilitate the sharing of information following an incident. If the consequence management powers do proceed, then we recommend defining what constitutes a secondary incident as an additional safeguard mechanism.

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions

Revising the protected information definition such that entities are encouraged to take a harm-based approach when disclosing information under the SoCI Act provides clarity and consistency for entities. We support simplifying how government and industry shares information during a crisis, where it does not impinge on our obligations under other legislation and where safeguards remain for the disclosure of such information.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

The telecommunications sector has a long history of working with government on strengthening an entity's cyber security posture (for example, through the Telecommunications Sector Security Reforms (TSSR)). We are well placed to continue this positive engagement and do not foresee the need to use the proposed review or remedy powers.

We understand the intention behind the proposed legislative change is to enable the Secretary of Home Affairs or a relevant Commonwealth regulator to direct a critical infrastructure entity to address deficiencies in that entity's Critical Infrastructure Risk Management Program (CIRMP). If these powers are used with appropriate oversight mechanisms and notice is provided to the necessary entities, then in our view it could improve the cyber uplift capacity across economy and foster greater resilience.

However, we query how wilful non-compliance will be determined and whether there have been instances that necessitate the introduction of such powers. We consider most entities operating under the SoCI Act understand risk management and the serious nature of their obligations, in upholding and protecting national security and act in good faith.

Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SoCI Act

We have actively participated in the Australian Telecommunications Security Reference Group (**ATSRG**).

We support combining the existing and proposed telecommunications security obligations into a single coherent framework under the SoCI Act. This means more than simply lifting each existing (or proposed) obligation (and associated penalty) and placing them all in the SoCI Act. The obligations need to work together to achieve improved security outcomes and should be considered within the context of the SoCI obligations of other critical infrastructure sectors. For example, many of the directions and information gathering powers under the TSSR already exist in the SoCI Act, and the TSSR penalties are significantly higher.

We will continue to engage with the ATSRG and Government to ensure these changes are proportional, effective and provide the sector with greater clarity about its obligations.