Parliamentary Joint Committee on Intelligence and Security Review of the Cyber Security Legislative Package

Telstra Response

25 October 2024

Introduction

Telstra welcomes the opportunity to respond to the Parliamentary Joint Committee on Intelligence and Security's (**PJCIS's**) Review of the Cyber Security Legislative Package.

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, businesses and the Government. We are a strong supporter of industry and Government collaboration and threat sharing and we will continue to work alongside the Australian Government on both operation security and cyber policy issues.

We acknowledge the important role that industry-government consultation has in shaping and designing reforms to address gaps in the existing regulatory framework and to strengthen our cyber shields to better protect individuals and businesses.

Telstra has actively engaged in earlier consultations on the Department of Home Affairs 2023-2030 Cyber Security Strategy Legislative Reforms. We look forward to continuing to engage with Government on the development of the Telecommunications Security and Risk Management Plan Rules.

Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill (SOCI Bill)

Enhanced Security Regulation for Telecommunications (Schedule 5 of the SoCI Bill / proposed new Part 2D of SOCI Act)

Telstra has consistently supported combining telecommunications security obligations into a single coherent framework under the Security of Critical Infrastructure Act (**SoCI Act**) and recommended that any changes should be proportional, effective and provide telcos with greater clarity about their obligations.

We welcome the proposed replacement of the TSSR with the Enhanced Security Regulation in Part 2D. We believe this change removes duplication and provides Industry with additional certainty around meeting the requirements.

However, it remains unclear to us why the penalties proposed under Part 2D for the telecommunications sector are disproportionately higher (7x) than any other penalties under the SoCI Act.

RECOMMENDATION 1: **We recommend that the penalties for Part 2D (Enhanced Security Regulations for the Telecommunications Sector) be proportional to the other penalties under the SOCI Act that apply to other critical infrastructure sectors.**

Data storage systems that hold business critical data (Schedule 1 of the SoCI Bill / proposed amendment to section 9(7) of the SoCI Act)

We welcome the proposed change to the definition of data storage systems to clarify that a secondary data storage system would only be considered part of a critical infrastructure asset where:

i. the responsible entity owns or operates the data storage system;
ii. the data storage system is used or is to be used in connection with the main asset;
iii. business critical data is stored or processed in or by the data storage system; and
iv. where impacts to that system could have a relevant impact on the main asset.

These are important limitations that prevent capturing systems that have no impact on Australia's critical infrastructure or national security.

Definition of critical telecommunications asset

The SOCI Bill amends the definition of critical telecommunications asset by removing the term 'facility' (defined in the *Telecommunications Act)* and replacing it with the term 'asset' (defined in the SoCI Act).

> ***critical telecommunications asset*** means:
> (a) a telecommunications network that is:
> (i) owned or operated by a carrier or a carriage service provider; and
> (ii) used to supply a carriage service; or
> (b) any other asset ~~a facility (within the meaning of the *Telecommunications Act 1997*)~~ that is:
> (i) owned or operated by a carrier or a carriage service provider; and
> (ii) used in connection with the ~~to~~ supply of a carriage service.

The EM explains that this is a consequential change, with the intent to remove ambiguity from the term 'facility' and to ensure that all assets used in connection with the supply of telecommunications services are captured by the definition. Telstra's view is that the term facility is well understood within the telecommunications sector and that no change to the definition is required.

However, if the Government does proceed with amending the definition of critical telecommunications asset, then this should not result in expanding the definition beyond telecommunications networks and other assets used in connection with the supply of a carriage service.

While this is the Government's intent, Telstra is concerned that in paragraph 269 of the Explanatory Memorandum, the current examples of assets that would now be captured as critical telecommunications assets potentially expands the definition and introduces ambiguity:

- *secondary data storage assets* (these should only be captured as critical telecommunications assets where they meet all of the criteria in section 9(7) of the SoCI Act, as amended by Schedule 1 of the SoCI Bill)
- *assets that don't directly make up part of a telecommunications network but support its function or are critical to carrying on a carriage supply business* (this example goes beyond critical infrastructure and potentially captures assets that may be used in connection with the supply of a carriage service but could not have any relevant impact on the functioning of a telecommunications network).

RECOMMENDATION 2: We recommend no change is made to the definition of critical telecommunications asset in the SoCI Act. If the definition is amended as proposed by the SoCI Bill, we recommend updating the Explanatory Memorandum to:

- **clarify that secondary data storage assets would only be captured as critical telecommunications assets where they met the criteria in section 9(7) of the SoCI Act; and**
- **removing the example about assets that don't directly make up part of a telecommunications network but support its function or are critical to carrying on a carriage supply business**

Telecommunications Security Risk Management Program

We welcome the opportunity in the coming months to continue to engage with Government on the Telecommunications Security and Risk Management Plan Rules, with a view to ensuring the risk management obligations are clear, proportionate and effective.