TELSTRA CORPORATION LIMITED

PJCIS REVIEW OF THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE PROTECTION) BILL 2022

Public submission

1 March 2022

01 Introduction

Telstra welcomes the opportunity to provide a submission in response to the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (**SLACIP Bill**). We support the Government's objective of the Critical Infrastructure and Systems of National Significance (**CI-SoNS**) reforms to uplift the security and resilience of the nation's critical infrastructure and have been an active participant in the consultation process for these reforms since mid-2020.

A key focus for us has been to avoid any unnecessary duplication between the proposed reforms and the existing security obligations contained in Part 14 of the *Telecommunications Act 1997*, the Telecommunications Security Sector Reforms (**TSSR**).

02 Feedback on the exposure draft and consultation process

Telstra provided a submission in response to the Exposure Draft and had several constructive discussions with the Department prior to its release. Our feedback focussed on concerns about regulatory duplication, clarifying the scope of the critical assets captured by the reforms and deconflicting obligations for assets that fall within multiple critical infrastructure sectors.

We've been active participants throughout the consultation process, including the sector specific workshops held in 2021 aimed at developing draft rules for the data storage or processing sector to underpin the Risk Management Program. We found the workshops to be productive and inclusive.

Telstra also attended each of the four town hall sessions on the SLACIP Bill hosted by the Department from December 2021 to February 2022. In our view, the discussions within the sessions were largely focussed on the Risk Management Program, with limited Q&A on the Enhanced Cyber Security Obligations or Systems of National Significance.

03 Has feedback been incorporated in the Bill or addressed in explanatory material?

Some key areas of feedback have been addressed in the SLACIP Bill. We support the amended definitions of *critical data storage or processing asset* and *critical telecommunications asset*. The amended definitions provide industry with much needed clarity about the scope of assets captured as critical infrastructure under these reforms. They also remove the issue of conflicting obligations for assets that fall within both sectors.

The SCLAIP Bill does not address our feedback about the consultation process prior to a System of National Significance (**SoNS**) declaration and liability protections. Section 52 of the Bill contemplates consultation with a responsible entity after the Minister gives notice of a proposed SoNS declaration. We recommend this be amended to also capture the engagement that will be required between the Government and a responsible entity before the Minister gives notice of a proposed SoNS declaration. In practice, the Government will need to closely work with an entity to adequately understand the impacts if an asset is compromised and the nature of any interdependencies with other critical infrastructure assets.

We also support extending statutory immunity for good faith compliance with *Security of Critical Infrastructure Act 2018* (**SOCI Act**) obligations to an entity's related company groups and contracted service providers. We are pleased to see these changes incorporated into the SLACIP Bill. In our view, there are some further anomalies that should also be addressed:

a) There is no provision in the SLACIP Bill which provides that an entity (or related group or contracted service provider) is not liable to action or other proceeding for damages in relation to an act done or omitted in good faith in undertaking a cyber security exercise.

b) There is no protection in the SLACIP Bill from liability for an entity that provides information in response to a systems information reporting notice or information gathering direction which is then misinterpreted and/or acted upon in a way that causes loss or harm.

c) While annual reports (Section 30AG), evaluation reports (30CQ/30CR) and vulnerability assessment reports (30CZ) are not admissible against an entity in civil proceedings relating to a contravention of a civil penalty provision of the Act (other than those provisions), there is nothing to prevent the reports being used in evidence in proceedings relating to penalties under other acts. There is also nothing to prevent the reports being used in evidence against officers, employees or agents.

d) There should also be a specific exemption for employees and agents of a responsible entity from having to give evidence in proceedings where they have assisted in the preparation of annual reports, evaluation reports, vulnerability assessments and systems information reports.

04 Recommendations from the Committee's Review Telecommunications Sector Security Reforms

As noted above, a key focus for us has been to avoid duplication between the proposed reforms and the existing security obligations TSSR. In this regard we welcome the recommendations of the Committee's *Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms*[1] particularly as they relate to non-duplication and to a closer collaboration and more candid exchange of threat sharing information between industry and Government.

We note that the Government has indicated it intends to achieve the policy objectives of a critical asset register and mandatory cyber security incident reporting through the Telecommunications Act and has already commenced consultation on a draft carrier licence condition to achieve this outcome.[2] We support this approach to ensuring these obligations are not duplicated for the telecommunications sector under the SoCI Act.

We would also support the establishment of dedicated telecommunications security threat sharing forum, to enable the Australian Security Intelligence Organisation and Australian Signal Directorate to brief telecommunications stakeholders about ongoing and emerging threats to the maximum classified level possible. As we noted in our submission to the Committee in that review, we believe the best security outcomes will be achieved by '*enhancing engagement and threat sharing between Government and the Communications industry*'.[3]

1 Parliamentary Joint Committee on Intelligence and Security, *Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms*, February 2022.
2 https://www.infrastructure.gov.au/have-your-say/security-information-obligations-carriers-and-eligible-carriage-service-providers
3 Telstra, *Review of Part 14 of The Telecommunications Act 1997—Telecommunications Sector Security Reforms*, 27 November 2020, p 2.