TELSTRA CORPORATION LIMITED

Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Public submission

1 February 2022

01 Introduction

Telstra welcomes the opportunity to provide a submission in response to the Exposure Draft (**ED**) of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (**SLACIP Bill**).[1] 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.

02 Removing unnecessary duplication for critical telecommunications assets

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**). We support the Government's recent decisions and proposed ED changes aimed at removing unnecessary duplication between the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) and TSSR for the telecommunications sector. We propose the following additional changes to help ensure this objective is achieved:

- Amending the Minister's proposed rules to enliven the positive security obligations in Part 2 and Part 2B of the SOCI Act, so that these obligations are applied to **critical data storage or processing assets** that are not a critical telecommunications asset.

- Simplifying the SOCI Act definition of **critical telecommunications asset** to provide industry with certainty about the scope of the critical assets captured by the CI-SoNS reforms and to ensure it is aligned with the assets captured by the TSSR.

2.1. Amended data storage or processing sector definitions to avoid a possible timing issue

Telstra strongly supports the ED proposal to amend the definition of critical data storage or processing asset to exclude any asset that is a critical telecommunications asset. This practical change removes the potential for conflicting obligations where an asset is captured within both asset classes.

However, to ensure this outcome is achieved, and critical telecommunications assets are not inadvertently captured, we recommend a corresponding change to the draft rules proposed by the Minister setting out the critical assets to which Part 2 and Part 2B of the SOCI Act will apply.

We recommend amending the rules so that these obligations be applied to critical data storage or processing assets that are not critical telecommunications assets. This will ensure the exclusion of telecommunications assets is effective even where there is a gap between the Part 2 and Part 2B obligations commencing and the definition of critical data storage or processing assets being changed in the SOCI Act.

2.2. Simplifying and aligning the definition of critical telecommunications assets

Telstra strongly supports the Government's decision to avoid unnecessary duplication by achieving key CI-SoNS obligations through the Telecommunications Act for critical telecommunications assets.

Security of the Telecommunications sector is already regulated by the TSSR. One of Telstra's key concerns about the CI-SoNS reforms was that it would create complexity and uncertainty for the

[1] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/exposure-draft-security-legislation-amendment-ci-protection-bill-2022

telecommunications sector by having critical telecommunications assets subject to duplicated or inconsistent obligations in both the SOCI Act and TSSR.

A remaining key inconsistency between the SOCI Act and TSSR is how critical telecommunications assets are defined. As drafted, the SOCI Act definition of critical telecommunications asset unnecessarily extends to non-critical assets and 'any other thing' used in connection with the supply of carriage services.

Telstra recommends resolving this inconsistency by amending the ED to replace the SOCI Act definition of **critical telecommunication asset** with the following:

> ***Critical telecommunications asset*** *means a telecommunications network or facility that is:*
>
> *(a) owned or operated by a carrier or a carriage service provider; and*
>
> *(b) used to supply a carriage service.*

Carrier, carriage service provider, telecommunications network and facility are already defined in the Telecommunications Act. This simplified definition better aligns with the TSSR and will provide industry and Government with certainty about the scope of critical telecommunications assets captured by the SOCI Act.

03 Enhanced Cyber Security Obligations and Systems of National Significance

We support the introduction of Enhanced Cyber Security Obligations (**'ECSO**') on assets of greatest importance to the nation. We welcome the Government's commitment in the Explanatory Document to continue to build on the strong voluntary engagement and cooperation already in place with critical infrastructure entities, with the ECSO being necessary in those instances where entities are unwilling or unable to voluntarily cooperate.

We also welcome recent comments about early engagement with entities as part of the SONS declaration process. To provide entities with additional clarity about this process, we recommend:

- Updating the consultation process in Section 52 of the ED to also capture the necessary consultation between the Government and an entity before a proposed declaration notice is issued to the entity in relation to a SONS.
- Updating the Explanatory Document to provide improved guidance on the application of the ECSO to SONS.

3.1. Consultation prior to the Minister declaring an asset a SONS

Section 52 of the ED appears to only partially reflect the SONS consultation process proposed by the Government. The ED contemplates consultation with a responsible entity after the Minister gives notice of a proposed SONS declaration. We recommend that Section 52 of the ED be amended to also capture the engagement that is required between the Government and a responsible entity before the Minister gives notice of a proposed SONS declaration.

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.

Based on prior consultation, to identify SONS, government and critical infrastructure entities could use a selection of high-impact scenarios (e.g., loss of financial services connectivity), as a means to identify all relevant systems that would contribute to the impact. Then an ISM-based threat/risk assessment could be conducted on these key systems and assets, looking at the likelihood, consequences, and impact for national security.

Section 52B provides that for the Minister to declare a critical infrastructure asset to be a SONS, they must be satisfied that the asset is of national significance. This requires the Minister to have regard to:

a) the consequences that would arise for:

   i. the social or economic stability of Australia or its people; or

   ii. the defence of Australia; or

   iii. national security;

if a hazard were to occur that had a significant relevant impact on the asset; and

b) any interdependencies the Minister is aware of between the asset and one or more other critical infrastructure assets; and

c) such other matters (if any) as the Minister considers relevant.

We believe prior consultation with an entity will be necessary before the Minister can be satisfied that an asset is of national significance.

3.2. Additional obligations apply only to SoNS

Part 2C of the ED provides that following a determination by the Secretary, one or more of the ECSO will apply to a responsible entity for a SONS in relation to:

a) the SONS; and

b) cyber security incidents.

While it is clear in the ED, this limitation of the ECSO to an entity's SONS asset is not entirely clear in the Explanatory Document. We recommend updating the Explanatory Document to make it clear that an ECSO doesn't extend to an entity's other critical infrastructure assets (or non-critical assets).

04 Liability protections

There are also several provisions in the ED that limit the liability of an entity's and its officers, employees and agents complying in good faith with CISONS obligations. We are of the view that some of these provisions, as drafted, do not provide sufficient protection. We propose aligning these provisions with the protections currently provided under the Telecommunications Act. For example:

- There is no provision in the ED 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.

- There is no protection in the ED 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.

- 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.

- 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.