TELSTRA CORPORATION LIMITED

DRAFT RISK MANAGEMENT PROGRAM RULES

Public submission

18 November 2022

01 Introduction

Telstra welcomes the opportunity to provide a submission in response to the Department of Home Affairs (**DoHA**) consultation on Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2022 (**Draft Rules**). We support the Government's objective to uplift the security and resilience of the nation's critical infrastructure and have been an active participant in the Critical Infrastructure and Systems of National Significance (**CI-SoNS**) reforms consultation process since it commenced in 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**). Accordingly, we support the Government's approach to implementing the critical infrastructure reform positive security obligations for the telecommunications sector through the Telecommunications Act.

We note that both the critical asset register, and mandatory cyber incident reporting obligations, have already been implemented for the telecommunications sector via a carrier licence condition for carriers (or a carriage service provider determination for nominated carriage service providers).[1]

02 Application of the Draft Rules

The Draft Rules will require responsible entities in a number of sectors (including the energy and data storage or processing sectors) to manage the impact of material risks to their critical infrastructure assets. The Draft Rules will not apply to critical telecommunications assets.

Responsible entities will need to maintain a risk management program that:

- Identifies each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset.
- Minimises the material risk of such a hazard occurring, so far as it is reasonably practicable to do so.
- Mitigates the relevant impact of such a hazard on the asset, so far as it is reasonably practicable to do so.

Each year, the entity will need to provide the DoHA with a Board-certified report on its risk management program. We support this all-hazards approach to risk management and believe that, while not articulated in the same way, that an all-hazards risk management approach is required by the TSSR's security obligation.

03 Risk management program rules for the telecommunications sector

We understand it is the government's intention to implement the Risk Management Program rules for the telecommunications industry via reform of the TSSR.[2] We support this approach and look forward to working with the DoHA and the Department of Infrastructure, Transport Regional Development, Communications and the Arts through the consultation process to achieve that reform.

---

1 Telecommunications (Carrier License Conditions – Security Information) Declaration 2022
Telecommunications (Carriage Service Provider – Security Information) Determination 2022.

2 Department of Infrastructure, Transport Regional Development and Communications, *Exposure Draft: 1. Telecommunications (Carrier License Conditions – Security Information) Declaration 2022; 2. Telecommunications (Carriage Service Provider – Security Information) Determination 2022Register of critical telecommunications assets and mandatory cyber incident reporting*, February 2022, page 6.
Department of Home Affairs, *Draft Risk Management Program Guidance for Industry*, 3 November 2022, page 8.