



TELSTRA CORPORATION LIMITED

REVIEW OF PART 14 OF THE TELECOMMUNICATIONS ACT 1997 TELECOMMUNICATIONS SECTOR SECURITY REFORMS

Public submission

27 November 2020



01 Introduction

We welcome the opportunity to provide comments on the Parliamentary Joint Committee on Intelligence and Security (PJCIS's) review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms (the TSSR).

The review comes as the Government is considering legislative changes to security requirements for critical infrastructure and systems of national significance (CI-SONS), including telecommunications networks and facilities. The Department of Home Affairs is currently consulting on an exposure draft of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill)* which will introduce new security and resilience requirements for owners of critical infrastructure through amendments to the *Security of Critical Infrastructure Act 2018 (the SOCI Act)*. We all want a secure and resilient nation and we welcome the Government's objective of uplifting the security and resilience of critical infrastructure through reforms that are appropriate and proportional.

We understand it is the Government's intention to introduce the Bill to Parliament before the end of the year prior to it being referred to the PJCIS for review. In implementing the proposed reforms, it is the Government's intention to prevent duplication of legislation and to leverage existing obligations wherever possible,¹ so we expect there will be significant overlap in the two reviews.

We support the use of the existing TSSR framework and believe there will be significant benefits in using it to meet the Government's objectives of strengthening the existing security of critical infrastructure framework. Accordingly, we anticipate that amendments may be required to the TSSR to align it with the requirements of the Bill. Considering this approach, we have outlined in this submission aspects of the TSSR that we believe should remain as drafted as well as highlighted areas that will require greater due diligence to ensure the two frameworks align.

02 The TSSR is an effective regulatory regime

We invest substantial resources to ensure they stand up to all threats and consider all hazards in our resilience and risk planning. We are supportive of the TSSR and have found the regime to be effective in meeting its goal of strengthening the security of Australia's telecommunications networks and facilities as well as enhancing engagement and threat sharing between Government and the Communications industry.

The TSSR introduced four key elements:

- **Security obligation:** All carriers, carriage service providers and carriage service intermediaries are required to do their best to protect networks and facilities from unauthorised access and interference.
- **Notification obligation:** Carriers and nominated carriage service providers are required to notify government of planned changes to their systems and services that could compromise their capacity to comply with the security obligation.
- **Information gathering power:** The Secretary of the Department of Home Affairs has the power to obtain information and documents from carriers, carriage service providers and carriage service intermediaries, to monitor and investigate their compliance with the security obligation.
- **Directions power:** The Home Affairs Minister has a directions power, to direct a carrier, carriage service provider or carriage service intermediary to do, or not do, a specified thing that is reasonably necessary to protect networks and facilities from national security risks.

Introduction of the TSSR did not change the way we consider and manage risk to our networks and facilities. Instead, it has introduced improved engagement and threat sharing with the Government on national security

¹ Department of Home Affairs, *Security Legislation Amendment (Critical Infrastructure) Bill: Explanatory Document*, p. 9.



risks which has provided an additional layer of threat awareness that informs our security assessment process and risk management decisions. We believe the engagement model with the Critical Infrastructure Centre has worked well for both Telstra and the Government. Two-way threat sharing has allowed Telstra to improve the quality of the threat information and detailed technical advice on which our risk assessments are based.

While the TSSR established formal communication requirements (notifications) between operators and the Critical Infrastructure Centre (CIC), in our view, the true benefit of the TSSR has been in improved collaboration and two-way information sharing that arose through less formal interactions, and the increased clarity that the CIC's guidance on specific proposed changes has provided for the teams building, managing and securing our networks and facilities. We would recommend that the informal engagement model be legislated into the TSSR and that formal notifications are used as a last resort mechanism where entities fail to engage with Government.

We recommend that the information gathering and direction powers under the TSSR remain in place and be carried into the sector specific rules under the proposed CI-SONS reforms. Whilst this regime has not been tested, the safeguards and guardrails were heavily negotiated during the TSSR implementation and should remain.

03 Proposed changes to the regulation of critical infrastructure

The Government has recognised the need to ensure the reforms are developed and implemented in a manner that secures appropriate outcomes without imposing unnecessary or disproportionate regulatory burden or duplication. We support the Government's intention to avoid duplication between the Bill and existing regulatory obligations such as the TSSR.

We suggest the PJCS recommend that the Government leverage the TSSR as far as possible to achieve the objectives of the Bill. To ensure consistency across regulations, this approach requires close consultation with the telecommunications sector to map the TSSR and SOCI obligations, address any 'gaps' within the TSSR framework and include clear criteria within the SOCI Act for 'switching off' duplicate obligations.

Should this approach be adopted by Government, we recommend the existing security obligation, information gathering powers and directions powers be retained within the TSSR and adopted under the proposed associated sector specific rules of the Bill to satisfy the requirements of the Bill's proposed Positive Security Obligation (**PSO**). We accept that the Bill's proposed PSO will take a more prescriptive approach to the matters that must be considered in meeting the PSO, we believe the existing security obligation of the TSSR does require adoption of an 'all hazards' approach and satisfies the overall intent and requirements of the PSO. We believe the objects of the PSO can be achieved by using (and perhaps, amending) the security obligation contained in the TSSR.

As a preliminary view we consider the following SOCI Act obligations would be most effectively captured under the TSSR obligations:

- The requirement for adopting and maintaining a critical infrastructure risk management program (Section 30AB and 30AH). The TSSR already includes the concept of a Security Capability Plan which we believe could be adapted to meet the required risk management program. If so, it might be appropriate to remove the notification obligations in the TSSR as the SOCI amendments do not include such notification requirements.
- Responding to Serious Cyber Security Incidents (Part 3A). We recommend these powers be precluded in respect of critical telecommunications assets and the Government rely on its directions and information gathering powers set out in Divisions 5 and 6 of Part 14 of the Telco Act.