TELSTRA CORPORATION LIMITED

Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*

Submission to the Independent National Security Legislation Monitor

13 September 2019

01 Introduction

Telstra appreciates the opportunity to make a submission to the Independent National Security Legislation Monitor's (the INSLM's) review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Act). We note the INSLM has been asked to report on the operation, effectiveness and implications of amendments made by the Act, and whether it:

- contains appropriate safeguards for protecting the rights of individuals;
- remains proportionate to any threat of terrorism or threat to national security, or both; and
- remains necessary.

As a major builder, supplier and operator of telecommunications networks and services, we are not well placed to answer the threshold questions of balancing the threat of terrorism or the threat to national security against appropriate safeguards for protecting the rights of individuals. We have very limited visibility of the threat assessment to Australia or its citizens and therefore believe these are matters for government, in conjunction with civil society, to determine.

We do, however, understand the challenges faced by law enforcement and national security agencies in relation to accessing clear communications and we share the Government's goal in ensuring law enforcement and national security risks are properly monitored and managed. We are also strongly committed to respecting the privacy and security or our customer's confidential information. Accordingly, we recognise the need to ensure regulation maintains an appropriate balance, in the public interest, and remains relevant and appropriate to support critical national security and law enforcement requirements in a rapidly changing social and technological environment.

The Act introduced a very broad set of discretionary powers which allow the agencies to seek assistance from a wide range of providers within the telecommunications supply chain (not just Australian based carriers and carriage service providers) and the manner or type of assistance to be provided can vary greatly. Introducing such a significant set of powers will necessarily involve a period of adjustment as the agencies and Designated Communications Providers (DCPs) begin operating under the framework. This is all the more so for DCPs which have not previously been subject to assistance obligations such as those applying to telecommunications carriers and carriage service providers under the *Telecommunications (Interception and Access) Act 1979* and under the 'reasonable assistance' provisions of the *Telecommunications Act 1997.* However, as an Australian carrier, which has always had obligations to assist Australia's law enforcement and national security agencies we have generally found the Act to be a workable evolution of our engagement with Australia's law enforcement and national security agencies. Nonetheless, we believe there remains room for improving the operation of the regime in the following areas:

- Limiting the potential for unintended consequences. For example, if a carrier is unknowingly using equipment or software which has been 'modified' as a result of a Technical Assistance Request (TA Request), Technical Assistance Notice (TA Notice) or Technical Capability Notice (TC Notice), this could result in an adverse impact to the carrier's network and its customers. There are two key issues here:
    - the secrecy provisions prevent the equipment or software vendor from advising a downstream carrier; and

  - while the immunity provisions protect the DCP who provided the assistance, there is no protection for providers in other parts of the supply chain which could be adversely impacted by their use of the 'modified' piece of equipment or software.

- Inclusion of an evidentiary certificate regime, such as the regime under the *Telecommunications (Interception and Access) Act 1979*, would assist in the efficient operation of the framework by allowing DCPs to issue a written certificate setting out facts in relation to the assistance provided.

- Allowing for commercial remedies against disclosure of information. The Framework provides confidentiality provisions to protect against disclosure of commercially sensitive information; however, there is no commercial remedy for a DCP whose confidential technical information has been compromised.

02 Protection from unintended consequences

The assistance and access framework covers the entire communications services supply chain, making it possible a TA Request, TA Notice or TC Notice could require 'modification' to a piece of network equipment or its operating software without the knowledge or awareness of other communications providers which deploy the equipment or software. For example, if a telecommunications provider (such as a carrier or carriage service provider) uses equipment or software supplied by a third party, that third party may have been separately required to provide technical assistance to an agency (potentially including the installation of software or equipment supplied by the agency) or to introduce new technical capability into their products.

Given the secrecy provisions of the framework, this could occur without the knowledge of the telecommunications provider and could result in an adverse impact to its network and/or its customers' use of the network. Such adverse effects could include service degradation, network faults, or other impacts on its business, or on non-target customers. While the immunity provisions of the framework would protect the DCP providing the assistance/capability under a TA Request, TA Notice or TC Notice, there is no protection for providers elsewhere in the supply chain if they (or their customers) are adversely impacted by the use of that 'modified' piece of equipment or software. Neither is there any provision for sharing of information or testing of modified equipment or software with the downstream DCPs to reduce the risk of unintended consequences.

To overcome these concerns, we believe the legislation should be amended to:

- Introduce a requirement to notify network operators (with an obligation on them to maintain secrecy) of a modification if there is a reasonable expectation the modification will be likely to adversely impact network performance. In some cases, it may be appropriate for agencies to consult not just with the third-party vendor, but also potential downstream DCPs, to properly assess whether the assistance being requested is in fact, reasonable and proportionate.

- Extend immunities which currently apply only to the communications provider given the request or notice, to any 'downstream' third parties affected by the request or notice.

03 An evidentiary certificate framework should be included

We believe the framework would benefit from the inclusion of an evidentiary certificate provision. An appropriately authorised employee of the relevant DCP should be allowed to issue a written certificate

setting out the facts of what has been done in providing assistance. Evidentiary certificates are intended to streamline the court process and reduce the costs imposed on a DCP by reducing the need to contact numerous subject matter experts to give evidence on routine matters. It also protects information on how capabilities were built and implemented from being revealed publicly, which would negatively impact the effectiveness of such capabilities. We note that the *Telecommunications (Interception and Access) Act 1977* contains such a provision and this could be easily adapted to the assistance and access framework.

04 Consideration should be given to commercial remedies

A TA Notice or a TC Notice may require a DCP to supply sensitive technical information, including software source code and service design documentation. Sharing this type of commercially sensitive information could, of itself, present a security risk if it ends up in the wrong hands. While there are provisions in the Framework obliging agencies to keep the information confidential (punishable by imprisonment), this will not provide a commercial remedy to a DCP if their information is compromised (e.g. if sensitive commercial information about upcoming product releases, upgrades or new features are disclosed).