OPTUS

Optus' Opening Statement

to

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

Review into the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018

WITNESS: Gary Smith, Head of Regulatory Compliance

DATE: Friday, 9 July 2021, 2.45-5.00pm

VENUE: Committee Room 2R1, Parliament House, Canberra – by videoconference

---

Optus welcomes the opportunity to contribute to the Committee's deliberations on the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (**the Bill**), which seeks to substantially amend the *Security of Critical Infrastructure Act 2018* (**the SOCI Act**).

The SingTel Optus Pty Ltd group of companies ("Optus") own and operate significant national telecommunications infrastructure and supply carriage and content services to a large portion of the Australian community. Optus takes its responsibility to provide competitive and secure communications services very seriously.

Optus agrees it should be a shared national endeavour between Government and critical infrastructure providers to increase the security and resilience of infrastructure critical to Australia's economic well-being.

In the short term, the proposed new critical infrastructure security laws are likely to add to the currently high commercial stresses on the communications industry. This is because the Bill only describes a high-level framework with the application of all key obligations determined by future Ministerial or administrative decision-making. Each one of these future decisions could add obligations which impose substantial cost or complexity. This means uncertainty exists over the final shape of the regulated landscape, and it is these final settings which will dictate the impacts on incentives to invest, commercial operations, and the level and timing of compliance costs.

The "framework" structure of the Bill also means that it is not currently possible to develop an informed view of the likely costs and benefits of the Bill.

To alleviate this situation Optus recommends that the Committee makes a finding that further consideration of the Bill should be deferred until the Government and Dept of Home Affairs provide a blueprint of the intended end-state regulatory scope and obligations, and the specific outcomes expected from the considerable decision-making powers delegated to the Minister and Secretary. Potentially regulated entities should be consulted and afforded the opportunity to provide input into the detailed blueprint.

OPTUS

Optus is also concerned about regulatory duplication and recommends the Telecommunications Act be adjusted to reflect the facts that the Bill is not being launched into a 'greenfield' legislative situation, and efforts should be made to dovetail it into existing security obligations provisions. As a minimum step, Optus recommends that the TSSR notification requirements in Division 3 of Part 14 of the Telecommunications Act should not apply to a responsible entity for critical telecommunications assets once it has been determined either that the entity is:

(a) subject to the positive security obligation which requires it to maintain a critical infrastructure risk management program; or

(b) operating a system of national significance.

Because the Bill outlines a high-level framework which leaves many of the important details to be determined by future processes and the application of various obligations to be decided by the Minister or Secretary, Optus believes the Bill should also contain suitable decision-making criteria, and rights for affected parties to be consulted and to seek review of certain decisions.

To further guide the broad scope of decision-making envisaged, Optus recommends more detailed statements of the regulatory objective be developed and added to the Bill. For example, Optus submits that the security objective should be balanced against the financial and administrative burden on the regulated entities which own and operate critical infrastructure. Our submission makes further suggestions.

Optus' submission also provides comment on the expansive nature of the definition of "critical communications asset", requesting it be reviewed to ensure it does not lead to the regulation of assets which are not required or necessary to support the 'real' critical infrastructure functions.

Clause 11 of schedule 1 of the Bill proposes to amend the definition of 'protected information' in the SOCI Act to be very broad, and to encompass just about all decisions or declarations made under the provisions of the Bill, including whether or not an entity and its assets have been declared as regulated entities - operators of critical infrastructure or systems of national significance. There are criminal and civil sanctions applying to the release of protected information outside of the limited exceptions outlined in the Act.

Optus is concerned that this specification and requirement to keep secure entire new classes of protected information leads to the emergence of new and substantial regulatory risk – civil and criminal sanctions are proposed for the disclosure of regulated information. This creates a complex situation both within the telecommunication supply chain, and in sectors where telecommunications services are a critical input into other critical infrastructure assets. This policy setting should be examined to provide some relief for situations where controlled disclosure, for example between regulated entities under suitable commercial and contractual terms, may lead to positive security outcomes.

I would be pleased to clarify any of the above points or respond to member's questions.

End.