Submission in response to consultation by the Department of Home Affairs on exposure draft:

Security Legislation Amendment (Critical Infrastructure) Bill 2020.

November 2020

EXECUTIVE SUMMARY

1. Optus welcomes the opportunity to provide comment on the consultation draft of 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 Bill, and the new regulatory regime it incorporates into the SOCI Act will have a significant effect on Optus' existing operations.

2. Optus also welcomes the fact that several issues it raised in response to the earlier consultation have been addressed by the Bill but notes there remains matters of concern which are set out further below.

3. 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 acknowledges the onus this creates to serve its customers and the community with competitive and secure services, and it takes this responsibility seriously.

4. Optus controls entities which are carriers, carriage service providers and content services providers and which operate in several of the proposed regulated sectors. 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

5. The proposed new critical infrastructure security laws are likely to add to the currently high commercial stresses on the communications industry. The Bill outlines a high-level framework which leaves many of the important details to be determined by future processes or decisions. This means a large measure of uncertainty will remain until well into 2021, and the policy and administrative settings which will dictate the impacts on incentives to investment, affect compliance costs and mitigate the risk of legitimate commercial endeavour being crowded-out will be unknown for an extended period.

6. The Bill should be dovetailed with existing regulatory provisions for the telecommunications industry. Optus recommends that policy and drafting adjustments be made so that the TSSR notification requirements in Division 3 of Part 14 of the Telecommunications Act do 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.

7. Optus believes while Part 3A provides some appropriate decision-making criteria and sets a suitably high bar for its use, it is appropriate that the exercise of these extraordinary authorisation and direction powers (such as the so-called step-in power) should be subject to an opportunity for independent review, and a requirement for the Minister and other decision-makers to have regard to submissions put forward by the affected critical infrastructure entity.

8. Optus recommends the Bill be amended to include additional objects for the SOCI Act, which articulate that the Act seeks to achieve a balance between the desired security and regulatory outcomes and the legitimate commercial interests of the regulated entities and sectors.

9. Optus recommends that a statement of regulatory policy be included in the Bill, which sets out an intention that both critical infrastructure assets and systems of national significance are to be regulated in a manner which does not impose undue financial and administrative burdens on the regulated entities which own and operate the infrastructure.

10. Optus is concerned that the expansive nature of important definitions will mean that the scope of the Bill is too broad, and it will consequently regulate assets which are not necessary for the support of 'real' critical infrastructure functions. For example, the definition of critical telecommunications asset includes any asset used 'in connection with the supply of a carriage service'. This could be anything from a network switching element to the audio-visual equipment in an ideation space through to a marketing database.

11. Optus is concerned at the emergence of new and substantial regulatory risk in the form of the civil and criminal sanctions which arise from the specification and requirement to keep secure entire new classes of protected information. This will drive administrative and governance cost. Efforts should be made to further limit the scope of protected information.

12. Optus recommends that the Bill be amended to include additional due process provisions around decision-making by the Minister and Secretary under Part 2A, Part 2B and Part 6A, including articulating:

    (a) Decision-making criteria, such as whether the decision might give rise to unreasonable financial or administrative burdens, have adverse impacts on incentives to invest or innovate, is technically viable, or could be reformulated to make a declaration more efficient or effective;
    (b) Opportunities for affected entities to make submissions prior to decision, to which the Minister must have regard;
    (c) The need to specify reasonable periods of time to implement requirements; and
    (d) A review or appeal process.

BACKGROUND

Optus' position as an Australian telecommunications carrier and carriage service provider

13. The SingTel Optus Pty Ltd group companies in Australia ("**Optus**") provides over 11 million services to the Australian community covering a broad range of communications services, including mobile, national, local and international telephony, voice over IP, fixed and mobile broadband, internet access services, subscription and IP television, and content services.

14. To deliver these services, Optus owns and operates fixed, mobile and long-haul transmission and access networks and the largest Australian fleet of satellites. These infrastructure assets provide a set of advanced technology platforms for the delivery of content and carriage services. Optus also has an extensive wholesale business, providing network services to many other carriage service providers.

15. General telecommunications carrier licences have been issued by the ACMA in relation to network units owned and operated by the following Optus group companies:

    (i) Optus Networks Pty Limited

(ii) Optus Mobile Pty Ltd
(iii) Optus Vision Pty Limited
(iv) Uecomm Pty Limited
(v) Optus Fixed Infrastructure Pty Ltd
(vi) Uecomm Operations Pty Limited
(vii) Optus Satellite Network Pty Ltd

16. Optus has the following group companies which operate as carriage service providers (as defined is the Telecommunications Act 1997):

(i) Optus Networks Pty Limited
(ii) Optus Mobile Pty Ltd
(iii) Optus ADSL Pty Ltd
(iv) Optus Internet Pty Ltd
(v) Optus Wholesale Pty Ltd
(vi) Uecomm Operations Pty Ltd
(vii) Optus Satellite Pty Ltd
(viii) Optus Mobile Migrations Pty Ltd

Optus' position as a satellite provider

17. Optus owns and operates Australia's premier satellite fleet, which is used to provide broadcast capabilities for both subscription and free to air television services and a range of other satellite-based services. Optus continues to invest in new satellite infrastructure to expand the technical capability and flexibility of its satellite services, and the capacity they provide to the Australian community for the distribution of content services and other communications services.

Optus' position as a content provider

18. Optus is a national provider of content services to the public in Australia, including services delivered via subscription TV, internet streaming, mobile applications and satellite delivery technology.

19. Optus' content services provide the Australian public with access to a range of premium sports and entertainment content, including Optus Sport (which provides live and on-demand coverage of international football properties such as Premier League, UEFA Champions League and J.League), Apple Music, and the Fetch and Optus TV featuring Foxtel subscription television services.

20. Optus holds subscription television licences under the Broadcasting Services Act for its broadcast of the Optus Sport channels via satellite television and its broadcast of the Optus TV featuring Foxtel service.

Optus' position in the Corporate and Government business market

21. Optus Enterprise is a part of the Singtel Group Enterprise business unit which serves corporate and Government customers in Australia with a range of sophisticated business services – including data services, mobility services and managed ICT services. It has major customers in the finance and government sectors and a range of other major corporate clients. One of the successful and growing pillars of its business model is the provision of a range of innovative and valuable cyber security services.

Summary

22. **Optus is the owner and operator of significant national communications infrastructure, and the supplier of important carriage and content services to a large portion of the Australian community. Optus acknowledges the onus this creates to serve its customers and the community with competitive and secure services, and it takes this responsibility seriously.**

23. **Optus sees it as 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.** Optus recommends that this spirit of shared endeavour should infuse the way the Government and the Parliament address the challenge and imperative of further developing the Bill and co-operative approaches between Government and the private sector.

THE BILL SHOULD NOT DUPLICATE EXISTING TELECOMMUNICATIONS ACT SECURITY REQUIREMENTS

24. Suitable transition arrangements should be included in the Bill to facilitate integration of the new critical infrastructure security requirements alongside the existing security regime which applies specifically to the communications sector via the Telecommunications Act. The Bill is not being launched into a 'greenfield' legislative situation and it should be dovetailed with existing provisions.

25. The requirement in the new regime for certain entities to have a regulated critical infrastructure risk management program should be an alternative to the operation of legacy provisions, rather than an additive requirement. In particular, the notification provisions of the Telecommunications Sector Security Reforms (TSSR) at Division 3 of Part 14 of the *Telecommunications Act* are, in effect, made redundant for critical infrastructure providers which are declared subject to the positive security obligation.

26. Because a TSSR notification only deals with an incremental change to infrastructure (and requires a risk and mitigation analysis) it relates to a sub-set of the matters required to be considered by the broader scope of regulated critical infrastructure risk management programs which form part of the proposed positive security obligation. The positive security obligation requires an entity to prepare and comply with an all-hazards risk assessment and mitigation plan - the defined 'critical infrastructure risk management program' - for its critical infrastructure operations. It also requires that the program be kept up to date, varied as required, signed off annually by the Board and reported to the regulator.

27. Maintaining the requirement for TSSR notifications in addition to the new regulated critical infrastructure risk management program obligations means critical infrastructure providers in the telecommunications sector will be subject to the cost and administrative burden associated with duplicative and overlapping regulatory regimes for no appreciative benefit. In addition, such an arrangement would place an unnecessary 'overlapping' burden on the resources of the Critical Infrastructure Centre which would have to deal with the bureaucracy of administering both arrangements.

28. Entities which provide critical telecommunications infrastructure should be exempted from the requirement to undertake TSSR notifications at the point when they are determined to be subject to the positive security obligation. This would provide a

straightforward transition path and a measure of integration between the legacy and new regimes.

29. **Optus recommends that policy and drafting adjustments be made so that the TSSR notification requirements in Division 3 of Part 14 of the Telecommunications Act do 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.**

30. This could readily be given effect by a minor amendment to the Bill and using existing provisions of Part 14 of the Telecommunications Act. For example, the exemption provisions available to the Communications Access Co-ordinator in section 314A(4) could be invoked by a decision of the Minister to include critical telecommunications assets operated by a responsible entity into the rules or a declaration as provided for in the proposed new section 30AB of the SOCI Act.

31. If appropriately specified, this approach could have the effect of allowing for a carrier or nominated carriage service provider to be exempted from the TSSR notification requirement in section 314(A)(1) by a companion decision taken by the Communications Access Coordinator triggered by the Ministerial decision to determine the assets are subject to the positive security obligation. Section 314A(5A) already provides that the Communications Access Co-ordinator may make such decisions at his or her own initiative. It would be an easy task to add the trigger of a Ministerial decision under the SOCI Act to initiate such an action.

COMMENTS ON THE CONTENT OF THE BILL

32. Clause 1 of Schedule 1 has the effect of removing a range of Ministerial decisions, i.e. those made under Part 3A of the SOCI Act, from the ambit of the *Administrative Decisions (Judicial Review) Act 1977*. This means the parties affected by such Ministerial decisions will not have the opportunity to seek judicial review whether the Minister followed due process in taking such decisions.

33. The decisions enabled by the proposed Part 3A of the SOCI Act are the critical set of decisions relating to Ministerial authorisation and a cyber security incident, including whether:

    (a) such an event has occurred, is occurring or is imminent;

    (b) the Minister is satisfied that the event is having an impact on a critical infrastructure asset;

    (c) the event will materially affect Australia's interests (social and economic stability, defence or national interest); and

    (d) that no other regulatory system can be used to respond.

34. If a Ministerial authorisation occurs under Part 3A, then a range of subsequent decisions may follow. Each of these decisions is also excluded from judicial review

by the effect of clause 1. Such decisions include Ministerial decision allowing the Secretary to issue various Directions to entities which own or operate critical national infrastructure or systems of national significance. These Directions may be:

(a) Information Gathering Directions (under s35AK);

(b) Action Directions (under s35AQ); and

(c) Intervention Requests (under s35AX)

35. The exclusion of these various decisions from review under the *Administrative Decisions (Judicial Review) Act 1977* means that the Bill does not afford a mechanism to review and confirm that due process was followed in the exercise of these decisions. A number of important criteria or pre-requisites are set out in Part 3A for the exercise of these Ministerial powers, but it is not clear how or whether there is any practical opportunity for review or oversight of the exercise of these Ministerial powers and any subsequent Directions issued by the Secretary under the authorisations.

36. The decisions under Part 3A and related decisions entail potentially very intrusive powers, which require the exercise of finely balanced judgement in complex circumstances. They should be informed by a suitable range of evidence and due process should be followed. In particular, to exercise powers in Part 3A, the Minister must form a view that:

(a) the issuing of information gathering Directions would facilitate a practical and effective response (proposed section 35AB(6)),

(b) the issuing of an action direction would satisfy the ten important pre-requisite conditions listed in the proposed 35AB(7), (8) and (9). These include substantial matters such as whether the directed entity is unwilling or unable to respond, whether the required action is technically feasible, reasonably necessary and a proportionate response. The Minister must also have regard to the impact of the directed activities on the entity and the consequences of compliance.

(c) the issuing of an intervention request has regard to the matters referenced in the proposed 35AB (10), which includes whether relevant entities are unwilling or unable take reasonable steps to resolve the incident.

37. **Optus believes while Part 3A provides some appropriate decision-making criteria and sets a suitably high bar, it is appropriate that the exercise of these extraordinary authorisation and direction powers should be subject to an opportunity for independent review, and a requirement for the Minister to have regard to submissions put forward by the affected entity.**

38. Schedule 1, clauses 5 and 6 propose to amend the objects and summary statement about the scope of the SOCI Act, but the proposed amendments are deficient in that they do not recognise or address the baseline fact that an entire new regulatory regime is being bought into being by the Bill, one which will regulate substantial sections of the Australian economy. In effect, the Bill allows for the establishment of an entire new top-to-bottom regulatory framework – including new regulators with new powers – which will regulate critical sectors of the economy, but this outcome is not addressed or even referenced in the objects of the Act.

39. In a comparable context for the communications industry, the *Telecommunications Act 1997* includes a broad-ranging set of objects including recognition of the legitimate commercial endeavours of the regulated sector and their benefit to the community. For example, an extract from section 3 includes the following objects:

> *"(c) to promote the supply of diverse and innovative carriage services and content services;*
>
> *(d) to promote the development of an Australian telecommunications industry that is efficient, competitive and responsive to the needs of the Australian community;*
>
> *(e) to promote the effective participation by all sectors of the Australian telecommunications industry in markets (whether in Australia or elsewhere);*
>
> *(f) to promote:*
>
> *(i) the development of the technical capabilities and skills of the Australian telecommunications industry; and*
>
> *(ii) the development of the value-adding and export-oriented activities of the Australian telecommunications industry; and*
>
> *(iii) research and development that contributes to the growth of the Australian telecommunications industry;"*

40. The SOCI Act should include objects which recognise and seek to balance its inherent security objective with the legitimate commercial interests of the regulated sectors of the economy. These sectors invest in and operate critical national infrastructure and a prime objective of the Act should be to draw a satisfactory balance between the security objective and the challenge of maintaining suitable incentives to invest, not adding unduly to the cost profile of regulated entities, promoting innovation and seeking to have a competitive Australian economy in the interests of the community.

41. **Optus recommends the Bill be amended to include additional objects for the SOCI Act, which articulate that the Act seeks to achieve a balance between the desired security and regulatory outcomes and the legitimate commercial interests of the regulated entities and sectors.**

42. A coincident outcome of this lack of explicit recognition that the Bill establish a new and broad regulatory framework is that the Bill does not include a statement of regulatory policy. In a comparable context for the telecommunications industry, the *Telecommunications Act 1997* includes a statement of regulatory policy at section 4, which states:

> *"The Parliament intends that telecommunications be regulated in a manner that:*
>
> *(a) promotes the greatest practicable use of industry self-regulation; and*
>
> *(b) does not impose undue financial and administrative burdens on participants in the Australian telecommunications industry;*
>
> *but does not compromise the effectiveness of regulation in achieving the objects mentioned in section 3"*

43. Such statements of regulatory policy provide useful guidance to all participants in the regulated sphere and should serve as a touchstone to regulators and those afforded decision-making power by the new framework. The Bill confers discretionary decision-making powers to Ministers, Departmental Secretaries and other officers of the Commonwealth in several significant areas and such guidance, as well as suitable checks and balances on such decision-making power, should be included in the Bill.

44. **Optus recommends that a statement of regulatory policy be included in the Bill after the objects at clause 5, which sets out an intention that both critical infrastructure assets and systems of national significance which are defined by the SOCI Act or by decisions made under the SOCI Act, are to be regulated in a manner which does not impose undue financial and administrative burdens on the regulated entities which own and operate the infrastructure.** These entities have entirely reasonable expectations that their legitimate commercial interests should be recognised and given weight in both the enacting mechanism and decisions made under the new regulatory framework being imposed on them.

45. In clause 6 of Schedule 1 of the Bill, the introduction to the 'simplified outline of this Act' sets out that:

"This Act creates a framework for managing risks relating to critical infrastructure.

The framework consists of the following:"

46. These comments do not fully describe the scale or scope of what the Bill entails. The practical effect of the Bill is to impose a regulatory framework, a set of obligations on regulated entities, and grant administrative decision-making powers to establish new and further obligations on regulated entities, with the intention of requiring entities which own and operate critical infrastructure to enhance their security posture and manage risks to their security.

47. **Optus recommends that the language of the proposed 'simplified outline of this Act' at clause 6 of Schedule 1 be adjusted to recognise and articulate that the Bill is establishing a new regulatory framework to place obligations on regulated entities and assets, and it includes all the associated regulatory powers ranging from powers to seek information and issue directions through to extreme powers to step-in and take over systems of national significance.**

48. Clause 7 of Schedule 1 specifies important definitions, including an expansive definition of 'asset', 'business critical data' and 'critical telecommunications asset'. The approach of using all-inclusive definitions increases the risk of regulatory over-reach because the Bill will regulate assets, business operations, systems and activities which are not directly related to the provision of services from the critical infrastructure.

49. In a large telecommunications provider there are many assets used in sales, marketing, procurement, finance and management that will fall within the definition of "used in connection with the supply of a carriage service", but which are not significant or even mandatory to maintain the integrity or availability of the essential carriage service function in a cyber-attack situation. These will nevertheless be regulated, unless specially carved out by regulation. The definition is set out below:

critical telecommunications asset means:

(a) a telecommunications network that is:
  (i) owned or operated by a carrier; and
  (ii) used to supply a carriage service; or

(b) a telecommunications network, or any other asset, that is:
  (i) owned or operated by a carriage service provider; and
  (ii) used in connection with the supply of a carriage service.

Note: The rules may prescribe that a specified critical telecommunications asset is not a critical infrastructure asset (see section 9).

50. **Optus is concerned that the expansive nature of important definitions will mean that the scope of the Bill is too broad, and it will consequently regulate**

assets which are not required or necessary to support the 'real' critical infrastructure functions. For example, a carriage service provider may use a range of assets 'in connection with the supply of a carriage service' to provide marketing, customer service or administrative services, the absence of which would be inconvenient but would not prevent the baseline operation of the critical infrastructure asset.

51. **The all-inclusive approach to certain definitions, including the definition of critical telecommunications asset, places a substantial and difficult onus on future decision-making under regulation to limit the potential for regulatory overreach. These definitions also make it difficult to understand the intended regulatory scope from the face of the Bill.**

52. Clause 11 of schedule 1 amends 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 exceptions outlined in the Act.

53. This approach of applying both criminal and civil sanctions to protected information raises substantial regulatory jeopardy and risk to regulated entities. This risk and operational impact is currently extremely difficult to quantify and calibrate because so many aspects of the new regime are to be established by future decisions under the high-level framework.

54. **Optus is concerned at the emergence of new and substantial regulatory risk in the form of the civil and criminal sanctions which arise from the specification and requirement to keep secure entire new classes of protected information.**

55. **Optus is concerned that substantial new administrative and governance arrangements will have to be developed just to deal with the new protected information generated by the bureaucracy of the Bill. Many of the details of the scale and scope of these classes of information are not currently known because they will be specified in future decisions which the Bill delegates to the Minister, Secretary or other officers of the Commonwealth.**

56. The Bill at clauses 38, 39 and 66 delegates substantial power to the Minister to determine how, when and on which assets and entities very important aspects and obligations in the Act will be applied, including:

    (a) The Declaration of an asset to be a **system of national significance** (proposed section 52B); and

    the making of rules under section 61 of the SOCI Act, including rules which determine whether the responsible entity for an asset is:

    (b) subject to the proposed new Part 2A obligations which require it to prepare, adopt, maintain, update, review, comply and report annually in relation to a **Critical Infrastructure Risk Management Program**; and

    (c) subject to the various proposed new Part 2B obligations relating to the **notification of cyber security incidents**.

57. It is notable that the Bill does not set out any decision-making criteria to guide the Minister in the exercise of these powers, with the limited exception that in deciding to

declare an asset to be system of national significance, the Minister must have regard to the nature and extent of interdependencies between that asset and other critical infrastructure assets. Apart from this exception, the Bill does not propose to limit or guide Ministerial decision-making in any substantial way.

58. Given the magnitude of the implications of such Ministerial decisions, regulatory best practice principles suggest the Minister should be required to have regard to the possible consequences on the regulated entity or asset, and the 'precision' of the decision. For example, what impacts would such decisions have on the commercial viability of the entity, its incentives to invest and innovate and whether the description of the declared system of national significance (i.e. the regulated asset) accurately proscribes the smallest possible regulated footprint to achieve the desired result.

59. The Bill requires the Minister to consult with the responsible entity about a potential declaration of a system of national significance under proposed new section 52B by issuing a notice and providing a period time for submissions. However, there is no requirement for the Minister to set out key matters on which further information could be provided or on which submissions could usefully focus. No detailed decision-making criteria are articulated in the Bill which would guide submitters about the factors on which Ministerial decisions may hinge and on which submissions could further inform.

60. Under the terms of the proposed section 52C (2) the Minister must consider submissions, but in making the final declaration decision there is no requirement under the proposed section 52B (2) for the Minister to have regard to matters raised in submissions.

61. For the Ministerial decisions which invoke obligations under the proposed new Part 2A and Part 2B of the SOCI Act, that is, the decisions made via rules under section 61 of the SOCI Act, there is no articulation in the Bill of requirements for due process, consultation, decision-making criteria or review.

62. The Bill at clause 39 of Appendix 1 delegates substantial power to the Secretary to determine how, when and on which assets and entities some very important aspects and obligations in the Act will be applied, including the Part 2C Enhanced Cyber Security Obligations which:

    (a) Impose incident response planning obligations (proposed section 30CB);

    (b) Require participation in cyber security exercises (proposed section 30CM);

    (c) Mandate vulnerability testing (proposed section 30CU);

    (d) Require sharing of information or installation of capability as directed by various systems information notices (various sections of proposed Division 5, Access to Systems Information)

63. Once a Ministerial declaration is made under the proposed new Part 6A regarding a system of national significance, the construction of the Bill provides the Secretary with very substantial discretion whether to impose all, some or none of these Part 2C obligations. There does not appear to be any requirement in the Bill for the Secretary to consult with potentially affected entities, to accept submissions, to seek relevant information, to have regard to any specific decision-making criteria, to consider any appeal or be subject to any review of such decisions.

64. **Optus recommends that the Bill be amended to include additional due process provisions around decision-making by the Minister and Secretary under Part 2A, Part 2B and Part 6A, including articulating:**

(a) **Decision-making criteria, such as whether the decision might give rise to unreasonable financial or administrative burdens, have adverse impacts on incentives to invest or innovate, is technically viable, or could be adjusted to make a declaration more efficient or effective;**

(b) **Opportunities for affected entities to make submissions prior to decision, to which the Minister must have regard;**

(c) **The need to specify reasonable periods of time to implement requirements; and**

(d) **A review or appeal process.**

End.