Submission in response to consultation by the PJCIS on:

Part 14 of the Telecommunications Act: The Telecommunications Sector Security Reforms (TSSR)

November 2020

EXECUTIVE SUMMARY

1. Optus welcomes the opportunity to provide comment to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in relation to its review of the operation of Part 14 of the Telecommunications Act, the Telecommunications Sector Security Reforms (TSSR). The TSSR regulatory regime has had a significant effect on Optus' operations and it has had significant operational experience with the notification provisions of Part 14.

2. 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, consistent with the security obligation in Part 14, and it takes this responsibility seriously.

3. If the TSSR notification provisions are retained, Optus recommends that a clearer notification threshold be developed and adopted to remove ambiguity, limit compliance risk and create an easy 'bright line' to guide decision-making for providers.

4. Optus has reviewed the TSSR status of well over 150 projects and proposed changes over the last two years and submitted formal TSSR notifications for 36 of them. The time for the resolution of these notifications has varied between 30 days to eight months.

5. A comparison of Optus' data to the industry data provided in CIC's annual reports reveals that for the first two years of the TSSR scheme, Optus has provided just over fifty percent of the notifications generated by the entire industry.

6. This underscores the point that the ambiguity of the notification threshold may mean the scheme is not operating as intended. The threshold is apparently being interpreted in different ways by different providers, which is leading to this differential result in terms of the distribution of notifications made by industry participants. It certainly means Optus is likely to be wearing a disproportionate share of the 'regulatory burden' associated with the scheme.

7. Optus' experience suggests there is no easy way to predict in advance the best timing in a project's lifecycle for a TSSR notification. It is also difficult to see how this dilemma can be resolved or how the uncertainties raised could be minimised by additional regulation.

8. From Optus' experience, the arrangements for sharing risk and threat information from government to industry which were promised at the commencement of the TSSR regime have not been made available.

9. Optus considers it would be extremely helpful to providers if the CIC explicitly outlined in detail the risk assessment framework or security standards which it, and its partner agencies, use in the analysis of proposed changes included in TSSR notifications. Such knowledge would assist providers structure their notifications and risk assessments using common language, definitions and approaches to those used by CIC, and make the entire process more efficient.

10. Optus has no concerns to raise about the treatment of its sensitive and commercial information under the TSSR regime, including by the Critical Infrastructure Centre.

11. Optus' experience has been that the project-by-project TSSR notification process required by Part 14 has been disruptive to a number of its major projects over the last two years, and added time, cost and complexity to the delivery and execution of complex and commercially significant investment programs. It is unclear if security outcomes have been improved commensurately. This situation has occurred despite the CIC operating relatively effectively in the administration of the scheme. It appears many of the concerns are inherent in the baseline policy setting which requires notification of individual incremental changes to critical infrastructure.

12. 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 under the proposed new *Security Legislation Amendment (Critical Infrastructure) Act* that the entity is either:

    (a) subject to the positive security obligation and the requirement to maintain a critical infrastructure risk management program; or

    (b) operating a system of national significance.

13. 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**.**

BACKGROUND

14. The SingTel Optus Pty Ltd group companies in Australia ("**Optus**") provides over 11 million services to Australian consumers, 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.

15. 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.

16. In short, 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.

17. The ongoing operation and evolution of Optus' business and networks requires sustained investment in new technical and commercial capability. This means changes which are relevant to Part 14 considerations have been a regular event in Optus' business. Optus has been subject to the Part 14 TSSR regime in its entirety and is experienced in its operation. Decisions made by Government and the Critical Infrastructure Centre (CIC) under the regime have had a significant effect on Optus.

EVOLVING REGULATORY CONTEXT

18. The communications sector is currently subject to layers of regulation related to the security of networks, infrastructure and carriage services, the protection of the content of communications and the preservation of the confidentiality of information collected while supplying carriage services. These rules are set out in multiple pieces of legislation including the *Telecommunications Act* (especially Parts 13 and 14), the *Telecommunications (Interception and Access) Act*, the *Crimes Act*, the *Privacy Act* as well as obligations in a range of Industry Codes, Standards and Guidelines.

19. As part of its Cyber Security Strategy 2020, Government is proposing to introduce an entirely new and additional regulatory regime applying to critical infrastructure entities in eleven sectors of the economy, including telecommunications. The providers which are currently covered by the TSSR provisions are also in scope of these proposed new security laws.

20. In late November 2020, the Department of Home Affairs undertook a short consultation on a Bill to amend the Security of Critical Infrastructure Act, with a view to meeting the Government's objective of introducing the Bill into Parliament before the end of the year. If this timetable is achieved and earlier precedents are followed, the PJCIS will also be asked to review this Bill at the same time as it is considering matters under this current TSSR inquiry.

21. Regulatory best practice principles suggest that new law should be structured to minimise overlap, inconsistency and duplication with existing law. This task should be considered by the drafters of the Bill and those determining the underlying policy settings for security regulation applying to the telecommunications sector and other sectors of the economy. It will likely also fall to the PJCIS to consider this aspect, and potentially in relation to the existing TSSR rules and the potential new law.

22. This places the PJCIS in a challenging position in terms of its deliberations on this Part 14 inquiry because the relevant legislative landscape mid-stream is in the process of changing and could very well be substantially different by mid-2021. It will be difficult to calibrate recommendations regarding TSSR without also having better knowledge of the final state of the proposed new security of critical infrastructure law, including the various industry rules and security standards contemplated to supplement that new legislation.

23. Based on a number of assumptions about the content of the proposed *Security Legislation Amendment (Critical Infrastructure) Bill 2020* and whether it is going to be reviewed by the PJCIS, Optus will venture some suggestions later in this submission about steps which can be taken to minimise duplication and allow these two pieces of legislation to dovetail together efficiently.

COMMERCIAL CONTEXT

24. The Government's TSSR security guidance on 5G and so-called 'high-risk vendors' has had a dramatic impact on both the fixed and mobile sectors of the telecommunications market in Australia. As well as altering the fundamental dynamics of the telecommunications equipment supply chain in Australia the outcome of this guidance also altered Optus' market position, investment strategy, customer outcomes and network design and capability.

25. The confidential Attachment to this submission provides additional commercial-in-confidence information for the PJCIS about the impact of this TSSR decision on Optus and the current commercial context within which this consideration of security laws is taking place.

THE NOTIFICATION THRESHOLD

26. The notification trigger described in section 314A continues to be problematic for providers to work with and interpret consistently in an operational context. In effect, notification requirements apply if a proposed change *"….is likely to have a material adverse effect on the capacity of the carrier or provider to comply"* with its Part 14 security obligations.

27. The threshold for the application of the notification obligation requires the application of practiced judgement about how to interpret the "material adverse impact 'criteria. In practice, it is not possible to develop a clear cut and unambiguous set of decision-making rules and it creates a risk of both:

(a) Under-notification; and
(b) Over-notification

when viewed comparatively across providers and when considering the notifications decisions taken within the same provider.

28. The explanation of the threshold routinely given to providers is that the notification trigger must be viewed as if applying to the 'unmitigated risk' which arises from a change. That is, if the change is of a type which if not suitably mitigated would raise a material adverse risk to security, then the change must be notified so the TSSR process can be used to review the proposed risk mitigations. If this is the 'proper' way of interpreting the application of the rule it leads to a different outcome – over-notification – compared to the alternative.

29. The alternative view is that the rule requires the provider to form a view about the 'residual risk' arising from the proposed change. In effect, the provider forms a view on whether a material adverse risk to security arises from the change having regard to all the controls and risk mitigations measures it proposes to implement.

30. If this view prevails, and it is clearly available from a plain reading of section 314A, then comparatively fewer notifications will arise because no provider will knowingly implement a change which leads to a material adverse effect on security. In practice, a provider following this interpretation will conclude that its controls mitigate the risks and therefore the threshold for notification is not met in all but extreme circumstances or changes.

31. This highlights the decision-making conundrum faced by providers because the threshold is described in this way. Providers face a difficult interpretive and practical choice and one path might lead to relative under-notification and the other could lead to relative over-notification.

32. This uncertainty means that it is highly unlikely that providers are implementing the rules in the same way within their organisations, creating an unequal playing field for providers. Due to the confidential nature of the TSSR notifications, it is difficult for providers to engage in detailed industry discussions on this topic to ensure a consistent application of the rules.

33. **If the TSSR notification provisions are to be retained, Optus recommends that a clearer notification threshold be developed and adopted to remove ambiguity, limit compliance risk and create an easy 'bright line' to guide decision-making.**

Impact of an unclear threshold on the number of notifications and the efficacy of the scheme

34. For its part, Optus has analysed its network, IT (OSS and BSS) and product development programs over the last two years to determine if TSSR notification requirements have been triggered. This amounts to the analysis of a substantial number of proposed changes and Optus decided to notify a relatively large number of them.

35. **Optus has reviewed the TSSR status of well over 150 projects and proposed changes over the two years to 30 June 20120 and submitted formal TSSR notifications for 34 of them.**

36. The data contained in the Annual Reports[1] provided by the Critical Infrastructure Centre on the operation of the reforms shows that over the same two-year period up to 30 June 2020, the CIC received a total of 66 notifications.

37. **Comparing these two data points shows that for the first two years of the TSSR scheme, Optus has provided just over fifty percent of the notifications generated by the entire industry.** At no point did the CIC suggest that Optus' notifications related to changes which did not need to be notified.

38. While Optus has a substantial investment program, there is no reason to suggest that when compared to the total activity across all relevant carriers and carriage service providers in the industry, that it should be responsible for a dis-proportionately large volume of changes, or that the changes it made were disproportionately more risky from a security perspective than changes made by other players in the industry.

39. This underscores the point that the ambiguity of the notification threshold may mean the scheme is not operating as intended. It is apparently being interpreted in different ways by different providers, which is leading to this differential result in terms of the 'share' of notifications. It certainly means Optus is likely to be wearing a disproportionate share of the 'regulatory burden' associated with the scheme.

40. Several informal briefings and discussions have also been held with the Critical Infrastructure Centre, some of which have involved changes which have subsequently been notified, others not. These informal processes with CIC have been valuable and productive.

OPERATIONAL ISSUES

Timing of notifications

41. There is no prescribed requirement regarding the timing of a TSSR notification in the lifecycle of a proposed change. If a provider forms a view that a change must be notified under TSSR provisions, the next question it must consider is at what stage of

[1] [1] Telecommunications Sector Security Reforms 2019-20 Annual report, and Telecommunications Sector Security Reforms 2018-19 Annual report

the change process should the required TSSR notification be developed (with its required risk analysis) and then lodged with the CIC.

42. Optus has tried each of the timing options available, but our experience suggests there is no conclusively correct answer. The options, and some of the pros and cons associated with each include:

(a) Notify early in the lifecycle of the proposed change. This has the potential benefit of getting the matter considered and an outcome available at an early stage, that is, certainty can be obtained on TSSR requirements and they can be specified before contracts are set, budgets locked down and solutions refined. However, an early notification also risks the TSSR review process being inconclusive because there is not enough information available about the detailed solution design, final vendor selection, risk assessment and likely operational arrangements. If this occurs, then a follow-on notification may be required when those items are better known. In effect, two notifications may be required for the same project.

(b) Notify late in the lifecycle of the proposed change. This approach has the benefit of being informed by finalised solution designs and technology choices, vendor selection being completed (or at least shortlisted) and risk analysis being better developed. It could lead to a relatively rapid TSSR review. However, this approach also means the regulatory and commercial risk of the TSSR outcome remains with the project until a late stage. The TSSR guidance or risk mitigation could overturn a vendor selection choice, a solution design, or require a substantial additional control to be developed. Such an outcome could delay the project, undermine its business case or require contract variations in which the provider is in a disadvantaged position.

43. Optus' experience suggests there is no easy way to predict in advance the best timing in a project's lifecycle for a TSSR notification. It is also difficult to see how this dilemma could be resolved or how the uncertainties raised could be minimised by additional regulation.

Availability of threat information and information-sharing arrangements between government and industry

44. Optus has engaged in conversation and analysis with the CIC about risk and threat information in the context of specific TSSR notifications. This has been helpful to finalise individual notifications once that threshold has been reached.

45. **From Optus experience, the broader arrangements for sharing risk and threat information from government to industry which were promised at the commencement of the TSSR regime have not been made available.** Such risk and threat information has not been made generally available, and certainly not in a manner which informs in advance any specific TSSR notifications.

46. The extensive discussions Optus which was privileged to participate in with relevant agencies during the period in which the Government 5G guidance was being developed were a significant exception and a contrast to the more limited information sharing which has been more generally available for the balance of the period of operation of the TSSR regime.

Security of sensitive information

47. Optus has no concerns to raise about the treatment of its sensitive and commercial information under the TSSR regime, including by the Critical Infrastructure Centre. Strong processes and procedures have been followed to protect information and the CIC has been responsive to requests for confidentiality. Optus has been confident to provide relevant and detailed information to support its TSSR notifications and associated risk analysis.

TSSR Guidelines

48. The Guidelines and information material which the CIC has provided has been generally helpful and timely.

Security standards and risk frameworks

49. **Optus considers it would be extremely helpful to providers if the CIC explicitly outlined in detail the risk assessment framework or security standards which it, and its partner agencies use in the analysis of proposed changes included in TSSR notifications**. Such prior knowledge would assist providers structure their notifications and risk assessments using common language, definitions and approaches, and make the entire process more efficient.

50. The absence of this information has meant that some TSSR notifications have had to be re-worked or have been subject to extensive questions coming back from the CIC to clarify aspects of the notification. With the mandated timeclocks in place for such additional steps in the process, the time this work consumes can quickly accumulate into significant delay in the context of a priority projects in a provider's investment schedule.

Uncertainty is the outcome of TSSR notification provisions

51. Optus' experience over the last two years has been that the TSSR notification rules and their operation has created substantial uncertainty and regulatory risk over major components of its investment program for networks, IT and products over the last two years.

52. The regulatory risk and uncertainty may, perhaps, be unavoidable with policy settings which require a Government notification and risk review procedure (based on unknown criteria) to be injected into the middle of the large, fast moving and technically complex procurement and investment processes which are associated with a competitive and capital intensive industry like telecommunications. The changes and projects involve cutting edge technology, global supply chains and stringent legal and governance processes to make investment decisions, manage commercial risk and schedule their delivery.

53. While the process has some mandatory decision-making timeframes, it is not uncommon for the end-to-end process of a notification to cumulatively span a number of these mandatory periods and exceed 90 days.

54. The commercial uncertainty and risk arising from the TSSR notification process has manifested in multiple ways:

    (a) Difficulty in interpreting the notification threshold (compliance risk);
    (b) Complexity in finalising the contracts with vendors for major projects or infrastructure;

(c) Choosing the correct time to lodge a TSSR notification
(d) Correctly specifying all business and security requirements for major tenders
(e) Agreeing how to quantify or calibrate TSSR risk in tender evaluation and decision-making
(f) Establishing clear risk assessment and risk analysis guidelines for both project delivery and for the preparation of TSSR notification documents
(g) Predicting the final cost of major projects
(h) Establishing predictable delivery schedules for major changes and estimating what time duration to allow to obtain TSSR guidance
(i) Understanding whether the current policy and control environment will measure up against the (unknown) risk assessment and security criteria applied in a TSSR review process
(j) identifying potential security requirements arising from leading edge technology and incorporating them into current deployments, or scheduling their adoption as technology matures
(k) whether scheduling can be arranged efficiently to marshal the technical, security and vendor resources at critical times to support efficient TSSR documentation and subsequent technical clarifications about a notification
(l) Achieving a clear understanding of the supply chain impacts of TSSR requirements, e.g. on vendor choice or suitable location of vendor development and support services

55. Optus' experience has been that the project-by-project TSSR notification process required by Part 14 has been disruptive to several of its major projects over the last two years, and added time, cost and complexity to the delivery and execution of complex and commercially significant investment programs. It is unclear if security outcomes have been improved commensurately. This situation has occurred despite the CIC operating relatively effectively in the administration of the scheme. It appears many of the concerns are inherent in the baseline policy setting of notifying individual incremental changes to critical infrastructure.

INTEGRATION OF TSSR AND THE *SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020*

56. Depending on assumptions about the progress of the Bill, it may be open to the PJCIS to consider suitable transition or integration arrangements between the new critical infrastructure security laws and the Part 14 TSSR requirements.

57. 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 existing provisions, rather than an additive requirement. It could be considered that the TSSR notification provisions are, in effect, made redundant for critical infrastructure providers which are declared subject to the positive security obligation.

58. 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 a regulated critical infrastructure risk management programs which form part of the proposed positive security obligation in the new regime. 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.

59. 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.

60. The policy response to this could be to remove the Part 14 TSSR notification provisions as a consequential amendment attached to the new *Security Legislation Amendment (Critical Infrastructure) Bill 2020.*

61. Alternatively, 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.

62. **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.**

63. 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 provide for in the proposed new section 30AB of the SOCI Act.

64. 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.

End.