Submission to Parliamentary Joint Committee on Intelligence and Security

Security Legislation Amendment (Critical Infrastructure) Bill 2020.

February 2021

EXECUTIVE SUMMARY

1. Optus welcomes the opportunity to provide comment 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 Bill, and the new regulatory regime it seeks to incorporate into the SOCI Act are likely to have a significant effect on Optus' existing operations.

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 communications and content services, and it takes this responsibility seriously.

3. 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

4. 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 remains over the policy and administrative settings which will dictate the impacts on incentives to investment and the level and timing of compliance costs. Uncertainty over the future course of regulation adds to commercial pressure on entities which are potentially within scope of the specific obligations of the Bill.

5. Optus recommends that the PJCIS make a finding that further consideration of the Bill should be deferred until the Government and Dept of Home Affairs provides 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 blueprint.

6. Optus recommends that the PJCIS requests the Government and Department of Home Affairs prepare a package for representation to Parliament which includes much greater specificity (even if via separate confidential report to Parliament and the proposed regulated entities concerned) of the:

   (a) Proposed key declarations and decisions – e.g. which companies are likely to be critical infrastructure entities, which assets are likely to be systems of national significance and what does a specification of a Critical Infrastructure Risk Management Program look like etc

   (b) Proposed regulatory settings – e.g. regulatory philosophy, intended competitive and investment outcomes, the regulator for each sector, methods of streamlining and reconciling conflicts between sectoral regulation and intentions to reduce over-lap with existing security regulation, recognition that the regime is aimed at fostering partnership and information sharing and is not designed to penalise and impose compliance obligations on industry.

1: BACKGROUND

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

7. 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.

8. 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.

9. General telecommunications carrier licences have been issued by the ACMA in relation to network units owned and operated by seven Optus group companies. Nine Optus group companies operate as carriage service providers (as defined is the Telecommunications Act 1997).

10. Optus group companies operate in at least three of the sectors the Bill proposes to regulate - space technology, communications, data storage and processing - and supplies or offers communications services to the eleven sectors the Bill seeks to regulate.

11. 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.

12. 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.

Structure of the following parts

13. Optus' key concerns about the high-level framework described by the Bill – what it does and does not contain - are set out in Part 2 of this submission. The overlay of the new regime onto the existing security settings for the communications sector is discussed in Part 3 and a significant recommendation is made about removing regulatory duplication. Further recommendations are made in Part 4 about some of the detailed regulatory settings in the Bill including certain checks and balances over delegated decision-making and the emergence of substantial regulatory risk arising from new classes of protected information – information about those same delegated decisions.

2: THE BILL SPECIFIES A HIGH-LEVEL FRAMEWORK - PROPER REGULATORY IMPACT ANALYSIS IS NOT POSSIBLE

14. **Optus recommends that the PJCIS advise the Parliament that further consideration of the Bill should be deferred until the Government and Dept of Home Affairs provides 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 blueprint.

15. In its current form, and without substantially more specific guidance, the potential costs and benefits imposed by the Bill on the Australian economy and regulated entities cannot be determined, nor is it possible to conclude whether the form of the Bill presents the optimal regulated framework and best solution to the security challenge which has been identified.

16. It is a reasonable request to Government to share the end-state regulated outcome which the high-level framework of the Bill is expected to produce. Such a view should have been developed to underpin the drafting of the Bill in its current form.

17. The absence of a more detailed blueprint of the intended end-state regulated outcome means the PJCIS and the Parliament is being asked to form a conclusion on a Bill which leaves just about all the important policy and operative details to be determined by future processes and decisions by the Minister and bureaucrats. On the information available, it is not currently possible to understand the intended future policy and administrative settings, and it is these settings which will dictate the impacts on incentives to invest in critical infrastructure, the commercial incidence on regulated entities, compliance costs, and significantly, whether the primary security objective can or will be achieved.

18. The lack of specificity about key obligations and settings foreshadowed in the Bill creates uncertainty which adds to the currently high commercial stresses on the communications industry and risks perverse impacts on incentives to investment, compliance costs and regulatory crowding-out of otherwise legitimate commercial endeavour. Government efforts to build the security posture of critical infrastructure should be designed to work co-operatively and co-exist with existing commercial activities also seeking to promote security outcomes for Australian business.

19. The Bill does not provide certainty on key aspects which need to be understood to determine whether it meets regulatory best practice. In particular, it is uncertain on the face of the Bill to conclude:

    (a) **Who is being regulated?** By examining the Bill, it is not possible for Optus to determine with certainty the extent to which it will be regulated, and if it is in scope, which of its corporate entities will be the subject to the regulated obligations. Optus operates seven licenced telecommunications carrier entities, nine carriage service provider entities as well as content service provider entities.

(b) **What scope of business assets and operations is being regulated?** The current definition of critical infrastructure appears so broad as to include business operations and assets not materially relevant to the security of that infrastructure. It is unclear whether this is the intended scope, or whether the uncertainty will be clarified by future Ministerial decision-making.

(c) **Which obligations will apply**? By examining the Bill, it is not possible for Optus to determine whether it will be subject to the obligations which apply to assets which are declared a 'system of national significance'. There is a material difference between these obligations and those applicable to assets or entities which are not declared.

(d) **What the obligations mean in practice**? The Bill contains the name and summary information about the various obligations, but specificity about the practical workings, expectations and requirements is to be determined by future processes.

(e) **Whether regulated entities will be consulted on the future design of the obligations:** the explanatory memorandum references the idea of "co-design", but the Bill does not reference or require consultation with (potentially) regulated entities on the design of details of important matters, for example, the form of a critical infrastructure risk management program.

(f) **The weight given to potential impacts on competition:** By examining the Bill it is not possible for Optus to determine whether consideration will be given to ensuring the incidence of regulation has an equivalent impact on its key competitors, or other sectors it competes with.

(g) **The weight given on incentives to invest and compliance costs?** the bill provides little specific guidance on the extent to which economic impacts on the newly regulated sectors should be given weight in decision delegated to the Minister and Secretary. This is important given the national economic imperative to preserve incentives to invest in critical infrastructure that will be vital to economic security of Australia. A prime objective of the Bill should be to draw a satisfactory balance between the security objective and the challenge of maintaining suitable incentives to invest.

(h) **Whether the rules can and will apply consistently across sectors?** Optus operates in several of the regulated sectors (e.g. space technology, communications, data storage and processing) and it is unclear whether differential or co-ordinated obligations will apply to each of these sectors, and how obligations will be applied to entities which straddle several sectors.

(i) **How will potential conflicts in supply chain obligations be managed?** Optus offers or supplies services to all the eleven regulated sectors. No information is available in the Bill about how alignment will be achieved, or conflict resolved, between the obligations as they are designed to apply to the communications sector each of the others sector. Will the practical effect be that Optus and other full-service communications providers have to comply with (and reconcile differences between) the detailed obligations devised for each of the eleven sectors?

(j) **How the Bill will co-ordinate with existing security regimes applicable to the communications sector?** The communications sector is subject to significant security rules in Parts 13 and 14 of the Telecommunications Act which should be removed to reduce overlap and duplication with the Bill. See further comment on this matter below

(k) **Who will be the regulator for each sector?** By examining the Bill, it is not possible for Optus to determine which agency will be designated as the regulator for each of the sectors in which it operates.

(l) **Whether the regulatory objects of the Bill should be more broadly balanced**: while the security objective is described, it is not placed in an overarching national context. Optus recommends the Bill be amended to include regulatory objects, which articulate that the Act seeks to achieve a balance between the desired security outcomes and the legitimate commercial interests of the regulated entities and sectors to invest in critical infrastructure. Further, the objects should state that the Bill should be administered in a manner which promotes that balance.

(m) **What regulatory philosophy will be applied to the administration of the Bill**? The Bill does not describe a regulatory philosophy which should be applied, and so regulated entities are provided little comfort that their legitimate commercial interests will be recognised and given weight in both the administration of the Act and decisions made under the new regulatory framework. Guidance should be provided in the Bill that the intention is that regulation does not impose undue financial and administrative burdens on the regulated entities which own and operate critical infrastructure. This would recognise the oft-stated approach that achieving better security outcomes is a shared endeavour between Government and the private sector.

(n) **Whether reasonable implementation periods will be allowed for the various obligations in the Bill**? The Bill imposes an entire new regulatory regime on key sectors of the economy. It will require regulated entities to undertake a substantial amount of work (the detail of which is currently unspecified) and the Bill does not articulate the imperative for reasonable implementation time to be built into the new set of obligations to allow for budgeting, planning and building any required new capability.

20. Optus' concerns with the Bill are focussed on both what the Bill does include and what it does not include. The Bill provides a high-level and internally consistent framework but it (nor the accompanying guidance material) does not provide potentially regulated entities with adequate information about the operation of the regime or the detailed obligations.

21. Optus submits that much further information – a more detailed blueprint of the key obligations, regulatory players and required actions – is necessary to allow a reasoned evaluation of whether the Bill is adequate. Only then can better informed opinions be formed about what additional matters should be addressed in the Bill itself or delegated to administrative decision-making. At this stage, the cost and benefit equation underlying the Bill is opaque and not available for evaluation.

22. It is these factors which lead Optus to recommend that the PJCIS advises the Parliament that further consideration of the Bill should be deferred until the Government and Dept of Home Affairs provides 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 blueprint.

23. Because these matters are so uncertain and broadly based, Optus has not sought to provide specific drafting suggestions on the Bill.

24. **Optus recommends that the PJCIS requests the Government and Department of Home Affairs prepare a package for Parliament which includes much greater specificity (even if via separate confidential report to Parliament and the proposed regulated entities concerned) of the:**

    (a) **proposed key declarations and decisions – e.g. which companies are likely to be critical infrastructure entities, which assets are likely to be systems of national significance and what are the detailed requirements for a Critical Infrastructure Risk Management Program, how often will cyber security exercises be run, what does reporting to ASD involve and when is it required etc.**

    (b) **proposed regulatory settings – e.g. regulatory philosophy, intended competitive and investment outcomes, the regulator for each sector, methods of streamlining and reconciling conflicts between sectoral regulation and reducing over-lap with existing regulation.**

3: CO-ORDINATION WITH THE EXISTING SECURITY REGIME APPLICABLE TO THE COMMUNICATIONS SECTOR

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. **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.**

31. 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.

32. 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.

4: DETAILED COMMENTS ON THE BILL

33. 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.

34. 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.

35. 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)

36. 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.

37. 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.

38. **Optus believes while Part 3A of the Bill 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.**

39. 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.

40. 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;"*

41. 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.

42. **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.**

43. 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"*

44. 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.

45. **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.

46. 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:"

47. 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.

48. **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.**

49. 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.

50. 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).

51. **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.

52. **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.**

53. 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.

54. 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.

55. **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 and recommends the class of protected information be reduced to information relating to any decision which is determined (on a case-by-case basis) to raise extraordinary sensitivity to public disclosure.**

56. **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.**

57. 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**.

58. 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.

59. 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.

60. 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.

61. 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.

62. 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.

63. 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)

64. 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.

65. **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.