OPTUS

Submission to the
Department of Home Affairs

Response to Exposure Draft: Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Public Version

1 February 2022

INTRODUCTION

1. Optus welcomes the opportunity to provide a submission regarding Bill Two of the critical infrastructure security reforms. As the owner and operator of nationally significant telecommunications infrastructure these obligations, as well as the broader requirements under the reforms, are of great interest to Optus.

2. 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 (over 11 million customers). Optus owns the largest Australian fleet of satellites, which support both public telecommunications access and provide capabilities for the Australian Defence Force and National Emergency Warning System.

3. Optus has a longstanding commitment to working with the Australian Government on national security issues. Optus is proud of the role it plays in supporting the safety and security of Australians and takes its responsibilities in this regard seriously.

4. While Optus has provided feedback on practical aspects of the legislation, **we support the enhanced national security posture that the legislation aims to achieve**. We understand the ever-evolving challenge of cyber security and continue to strengthen our capacity to respond to modern threats.

5. To support the co-design process that Government is undertaking, we recommend four key areas where the legislation could be strengthened (further detail below):

   (a) **Refining the definition of critical infrastructure asset** as it applies to the telecommunications sector (as has been done with other sectors such as higher education);

   (b) **Engaging with entities likely to be designated as a system of national significance (SoNS) prior to implementing the mandatory cyber reporting obligations**. This will reduce duplication and promote a more coherent approach to cyber security obligations for potential SoNS entities.

   (c) **Extending consultation with potential SoNS to at least 45 days and consulting jointly with relevant entities**. This reflects the inherent complexity of SoNS entities and will produce better outcomes for both SoNS entities and Government.

   (d) **Establishing very clear and appropriate thresholds for the Government Assistance Measures**. While we appreciate Government has indicated a number of clear parameters for these measures during the consultation process, it is important that these are clearly defined in legislation.

6. Optus also recommends that the Explanatory Memorandum to the legislation makes it clear that industry is being asked to play a supporting role in achieving national security outcomes and that it is not intended for the regime to operate as a set of punitive compliance obligations.

7. Our sector has a strong track record of working collaboratively with government to meet Australia's national security needs. Optus is keen to continue this collaboration and we believe the best approach is to build on what is working well today.

8. Optus would welcome the opportunity to discuss any of these issues in further detail.

9. As a member of the Communications Alliance, Optus also supports the Communications Alliance submission.

SUBMISSION

Definition of Critical Infrastructure Asset Needs to be Refined

10. Optus operates the largest fleet of Australian satellites and the second largest telecommunications network in the country, supporting more than 11 million services. We own seven carrier entities and 11 carriage service provider entities that together provide a full suite of modern telecommunications services, including internet, content and mobile. In this context, Optus already has a mature risk management approach based on our understanding of the complexities of our network infrastructure.

11. We recognise, however, that Government will always have unique insights into certain threats or risks and is seeking to uplift resilience across a range of critical infrastructure sectors. Optus supports this goal and, to assist in achieving it, recommends that the definition of 'critical telecommunications asset' be refined so as to be more practical.

12. At present, the definition is:

    (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.

13. It is section (b) that is particularly problematic and **Optus recommends it be removed**. Especially in the modern era, the scale of assets that are "used in connection with the supply of a carriage service" is impracticably vast. Such a definition could plausibly include anything from billing systems to the vehicles used by maintenance staff.

14. As has happened with other sectors – such as higher education and data storage and processing – Optus recommends that the Government work with the telecommunications sector to refine this definition *before* the obligation to provide a register of critical assets is implemented. As it stands, the current definition is unworkable because it is so broad. Refining the definition will ensure the risk management programme can be properly focused on critical risks and implemented in a practical way. It will also reduce compliance costs and support Government by only capturing relevant assets.

15. We would welcome the chance to discuss a revised definition with Government.

Government Should Designate Systems of National Significance Before Implementing the Mandatory Cyber Reporting Obligations

16. At present, Optus understands that all critical infrastructure entities will be required to comply with the minimum cyber security obligations in the first instance. Following this, a smaller subset of entities will be deemed 'systems of national significance' (SoNS), which will impose 'enhanced cyber security obligations' on these entities. While Optus appreciates that these enhanced obligations are a 'menu' that will be selectively applied on a case-by-case basis, we also understand that where these enhanced obligations duplicate the intent of the mandatory reporting obligations, only the latter will apply.

17. It would therefore seem more practical to designate entities as SoNS *prior* to imposing the mandatory reporting obligations to avoid duplication and unnecessary compliance costs. For entities such as Optus that may be designated as a SoNS, there is a possibility that we will have to develop compliance processes for mandatory cyber reporting only to undergo a second round of compliance for the enhanced obligations (as well as reconciling any duplicative requirements between the two regimes).

18. Optus therefore recommends engaging with entities that are likely to be designated as a SoNS prior to implementing the mandatory cyber reporting obligations. This would support more timely, efficient and effective compliance from these nationally significant entities by undertaking a single, holistic compliance uplift.

Consultation with Potential SoNS Should be Extended and Aligned with Related Entities

19. In addition to the above, Optus recommends that the consultation period with potential SoNS be extended from 28 to at least 45 days. As outlined earlier, Optus operates a highly technical and complex modern telecommunications architecture. 28 days is entirely insufficient to consider and respond to the designation of an entity as a SoNS.

20. In addition, this consultation should occur with the interdependencies that sit at the heart of the SoNS concept itself in mind, i.e. that it should occur jointly with related sectors (e.g. telecommunications is heavily dependent on the energy sector). In many instances, ownership of some of the major risks that SoNS face will sit with these interdependent entities. Consultation should reflect this and allow both SoNS and the Government to consider risks and mitigations in a more holistic manner.

21. This is particularly the case in the absence of a clear definition of a SoNS. At present, all entities have to go on is the broad notion of whether a hazard experienced by the entity would have a material impact on Australia's socio-economic stability, national security or defence as well as the interdependencies between the entity and other critical infrastructure assets. Given this broad and vague definition, it is exceedingly difficult for entities to know whether they will be designated as a SoNS and prepare accordingly.

22. There is also uncertainty as to how exactly critical infrastructure assets are linked to the concept of a SoNS. At the moment, the Bill only states that the Minister must consider the interdependencies between a SoNS and other critical infrastructure assets, including "the nature and extent of those interdependencies". This guidance is vague and makes it impossible for entities to understand the precise considerations that will inform the designation of a SoNS and the specific obligations that will apply as a result.

23. Both Government and telecommunications entities will benefit from an extended consultation period as it will allow for a holistic and comprehensive consideration of the particular risks and obligations that apply to each entity. It will also help provide certainty about the full breadth of entities' obligations from the outset, rather than having to navigate an evolving regime of obligations in the initial implementation period.

Thresholds for the Government Assistance Measures Should be Defined in Legislation

24. Although we appreciate advice that the Government Assistance Measures are only intended for the most extreme scenarios, Optus strongly recommends that the thresholds for their use be enshrined in the legislation. Given the extraordinary and intrusive nature of these powers, it is vital that businesses have confidence regarding the parameters for their use. The legislation should clearly set out the thresholds that could trigger use of these measures, the safeguards for ensuring they are used appropriately and a mechanism for recourse in the event that unintended damage is done.

CONCLUSION

Optus supports the Government's plan to uplift the resilience of Australia's critical infrastructure. As a national telecommunications provider and operator of the largest satellite fleet in the country, Optus appreciates the need for security and we take our responsibilities seriously.

To support the Government in its efforts to improve security outcomes, Optus has four key recommendations regarding the critical infrastructure asset register and mandatory cyber reporting obligations:

1. **Refining the definition of critical infrastructure asset** as it applies to the telecommunications sector (as has been with other sectors such as higher education);

2. **Engaging with entities likely to be designated as a system of national significance (SoNS) prior to implementing the mandatory cyber reporting obligations.** This will reduce duplication and promote a more coherent approach to cyber security obligations for potential SoNS entities.

3. **Extending consultation with potential SoNS to at least 45 days and consulting jointly with relevant entities**. This reflects the inherent complexity of SoNS entities and will produce better outcomes for both SoNS entities and Government.

4. **Establishing very clear and appropriate thresholds for the Government Assistance Measures**. While we appreciate Government has indicated a number of clear parameters for these measures during the consultation process, it is important that these are clearly defined in legislation.