

OPTUS

Submission to the
Department of
Infrastructure, Transport,
Regional Development and
Communications

***Draft
Telecommunications
Declaration and
Determination 2022***

Public Version

March 2022

INTRODUCTION

1. Optus welcomes the opportunity to provide a submission regarding the *Draft Telecommunications (Carrier Licence Conditions – Security Information) Declaration 2022* (*‘the Declaration’*) and the *Draft Telecommunications (Carriage Service Provider – Security Information) Determination 2022* (*‘the Determination’*) – together *‘the Rules’*. Optus notes that the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (*‘Bill Two’*) is currently being reviewed by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The passage of this Bill would have implications for the Rules and Optus encourages further consultations following the publication of the PJCIS report and passage of Bill Two.
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 services). Optus also owns the largest Australian fleet of satellites, which support both public telecommunications access and provide important capabilities for the Australian Defence Force and National Emergency Warning System.
3. Optus has a longstanding commitment to and experience in supporting the Australian Government on national security issues. Optus is proud of the role it plays in supporting the safety and security of Australians and the critical infrastructure on which they rely and takes its responsibilities in this regard seriously.
4. Optus has **four recommendations** and suggests several areas for clarification:
 - (a) Allowing entities to **comply with the Rules at a group level** rather than for each relevant entity that they control.
 - (i) Optus, for instance, has seven carrier licences and eleven carriage service provider entities. Having to maintain separate asset registers and reporting processes for each of these would be incredibly complex, inefficient and ineffective.
 - (b) Ensuring that the Regulation Impact Statement process **allows sufficient time for accurate cost estimates to be developed**.
 - (c) **Limiting the incident reporting requirements** in section 10 to the impact on essential carriage services.
 - (d) **Providing scope for ASD officers to alter reporting timelines** under section 11 where warranted by the circumstances.
 - (e) Clarifying the following elements:
 - (i) how carriers will report the location of their assets
 - (ii) the reporting requirements for maintained data
 - (iii) how section 10(2) will interact with forthcoming ransomware legislation.
5. Optus would welcome the opportunity to discuss any of these issues in further detail.

Allow Compliance at a Group Level

6. As currently written, Optus understands that the Rules would require us to maintain separate asset registers and reporting processes for each carrier and carriage service provider that we control. At present, Optus holds seven carrier licences and controls 11 carrier service provider entities. Many assets are shared across entities. It would therefore be more practical if entities could maintain a single register that covered all relevant assets under their control as well as having a single incident reporting process.

Appropriate Time is Needed to Accurately Estimate Costs

7. At this stage, there are still a number of unknowns that make estimating the cost impact of the reforms difficult. It is not clear, for example, which entities will be designated as Systems of National Significance and what additional obligations will be placed on them (noting that the Government has indicated the options in Bill Two are a 'menu' that will be applied on a case-by-case basis). Optus (and many others across the range of critical infrastructure sectors) has expressed concerns in the past about the potential compliance costs involved in these reforms. Optus also notes that, to date, the Regulation Impact Statement (RIS) process has not followed agreed Government best practice (i.e. conducting a quantitative RIS prior to the introduction of legislation).
8. To address these concerns, Optus strongly encourages the department to **undertake a thorough RIS process before the Rules come into effect** to ensure accurate cost estimates can be developed and businesses can plan effectively.
9. Government should also consider providing funding to support any additional systems, processes or tolls that industry may need to implement to comply with the new requirements.

Incident Reporting Should be Limited to Carriage Services

10. Section 10 currently states that an incident has a 'significant impact' if:
 - (a) The asset is used in connection with the provision of essential goods or services; and
 - (b) The incident has materially disrupted the availability of those essential goods or services

In the context of the telecommunications industry, not only do we provide essential services, we support the provision of a wide range of essential goods and services in other sectors. From a reporting perspective, this potentially imposes an incredibly complex regulatory burden where we would have to provide information on the impact to various goods and services for which we do not have visibility. Optus therefore recommends that this section be limited to **essential carriage services**.

Reasonable Adjustments to Section 11 Reporting Timeframes Should be Permitted

11. The reporting requirements under section 11 allow for an initial verbal notification of an incident followed by a written report either 12 or 72 hours later depending on the nature of the incident. The draft Rules allow for an ASD officer to determine that no written report is required but does not allow them to alter the reporting timeframes. Optus can imagine circumstances where this initial notification could benefit from reasonable adjustments to these timeframes. We therefore recommend that ASD officers be given the authority to make reasonable adjustments to these reporting timeframes on a case-by-case basis.

Clarification Would be Welcomed in Several Areas

12. While Optus acknowledges that some elements of Bill Two are still subject to change, it would nonetheless be helpful if several elements of the Rules could be clarified.
13. The Rules currently require relevant entities to be able to provide operational information to the Secretary of Home Affairs in the event of an incident. Section 6(1)(a) defines one sub-set of this information as “the location of the asset”. In the event of a significant telecommunications outage, this could involve hundreds or, in extreme cases, thousands of individual assets. Primarily this would be individual towers but could also include numerous ancillary assets such as power generation facilities.
14. Given the large number of individual assets likely to be involved in a serious telecommunications outage, Optus proposes that multiple assets that are the subject of a report should be bundled together as one. Similarly, a reportable incident could involve assets such as a subsea or major fibre link cable which runs between multiple locations and the exact location of the incident along the route is not known at the time of the report. In this case, it should be acceptable to provide general details of the location or route at the time of initial notification, with more details to follow when available.
15. Similarly, Optus suggest further thought is required on how entities should report on arrangements for their ‘maintained data’ as required by section 6(1)(e). Again, this could involve a range of different data-sets that vary in size and scope. For example, Optus holds personal information on our millions of customers; we process a vast amount of data as part of monitoring and sustaining our infrastructure; and every day a huge amount of sensitive communications data traverses our network. This data is stored in many different ways and is not always going to be easily accessible in the event of a cyber incident. Reporting on the arrangements for how data is maintained is therefore very complex and warrants further discussions with affected entities.
16. Under section 10(2), a cyber security incident is only considered to have a significant impact if:
 - (a) The asset is used in connection with the provision of essential goods or services: and
 - (b) The incident has materially disrupted the availability of those essential goods or services.

In the event that a ransomware attack fell under the above definition, Optus seeks clarification as to how the requirements of these Rules would work in light of the parallel ransomware legislation being developed by the Commonwealth. Would entities have to report incidents under both Acts, potentially to two different points of contact in ASD? Would there be different reporting requirements between the two pieces of legislation? Optus would welcome the chance to discuss these and other questions about how these two pieces of legislation will interact.

CONCLUSION

17. 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.
18. We acknowledge that Bill Two is still subject to change and the Rules are therefore in early draft form. Optus thanks DITRDC for its early consultation on the Rules and a summary of our initial feedback is as follows:
 - (a) Allow entities to **comply with the Rules at a group level** rather than for each relevant entity that they control.
 - (b) Ensure that the Regulation Impact Statement process allows sufficient time for accurate cost estimates to be developed.
 - (c) Limit the incident reporting requirements in section 10 to the impact on essential carriage services.
 - (d) Provide scope for ASD officers to alter reporting timelines under section 11 where warranted by the circumstances.
 - (e) Clarify the following elements:
 - (i) how carriers will report the location of their assets;
 - (ii) the reporting requirements for maintained data;
 - (iii) how section 10(2) will interact with forthcoming ransomware legislation.
19. We would welcome the opportunity to discuss these issues in more detail.

[End of Submission]