OPTUS

Submission to the
Department of Home Affairs

# Response to Government Consultation Paper: Cyber Security Strategy Legislative Reforms

Public Version

March 2024

# EXECUTIVE SUMMARY

1. Optus welcomes the opportunity to provide a submission on the Government's cyber security strategy consultation paper.

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 owns the largest Australian fleet of satellites, which support both public telecommunications and provide crucial 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. It is proud of the role it plays in supporting the safety and security of Australians and takes its responsibilities in this regard seriously.

4. Optus welcomes the government's approach of genuinely co-designing the implementation of the cyber security strategy. We support many of the proposals put forward and offer the following broad comments in support of the co-design process:

   (a) The overarching goal of the implementation process should be to separate the processes for operational incident response from regulatory investigations;

      (i) Further explanation of this concept is provided in the body of the submission but the essential idea is that the technical incident response and consequence should take precedence and be separated (e.g. in terms of information-sharing) from any subsequent regulatory investigations.

   (b) Several definitions and thresholds would benefit from further clarity, including:

      (i) The parameters of the limited use obligation;

      (ii) The definitions for the data storage and processing obligations;

      (iii) The definitions and thresholds relating to the consequence management powers; and

      (iv) Thresholds for the review and remedy powers.

   (c) Further work is needed to demonstrate the need for and utility of both the consequence management powers and the Cyber Incident Review Board.

      (i) Optus notes, for example, that the step-in powers in Part 3A of the SOCI Act are yet to be invoked. The addition of an all-hazards consequence management power would therefore amount to a significant expansion of as yet unrequired powers.

5. In addition to these overarching comments, we have offered more specific responses to each proposed measure, including many of the questions in the consultation paper. We would welcome the opportunity to discuss any of these issues in further detail.

6. As a member of the Communications Alliance and Tech Council of Australia, Optus also broadly supports their respective submissions.

## OPERATIONAL AND REGULATORY RESPONSES SHOULD BE SEPARATED AND STREAMLINED

7. A challenge Optus experienced in responding to its cyber incident was having to provide extensive information to regulators while simultaneously dealing with the incident itself and any consequences it generates. While this information is just as important as the incident response itself, it is not as time-critical. Optus therefore suggests that the implementation of several measures be guided by a clear principle: separating the operational response to an incident from the regulatory response. In doing so, this separation should occur in both reporting timeframes and information-sharing protocols.

8. The most urgent requirement of a cyber incident is the immediate incident response itself. In the event of an incident that reaches a scale that would be relevant to the SOCI Act, the resources in both time and personnel involved in such a response are considerable. Having numerous information requests from regulatory bodies while simultaneously managing the incident itself places an unnecessary and counter-productive burden on the entity. To use an analogy, it is akin to asking firefighters to explain their firefighting procedures and identify the cause of a blaze whilst in the middle of extinguishing a bushfire.

9. Instead, Optus recommends that one legislative amendment under the strategy be a change in regulatory reporting timeframes to allow for an initial period where the entity can solely focus on the operational incident response and does not receive any formal information requests from regulatory bodies (beyond basic notification requirements). While each incident response time will vary, we suggest a useful time period should be at least one month.

10. This would not only benefit the entity by allowing them to focus entirely on incident response and consequence management for this period, it would also benefit regulators. It often takes several weeks to build up even a preliminary view of the nature of a cyber incident and how it might have occurred. Forming a complete picture (or as complete a picture as possible) about an incident can often take months or even longer. Allowing for this initial, short delay in regulatory investigation requests would therefore give an affected entity time to be able to provide more useful information to regulatory bodies.

11. In addition to this timeframe separation, Optus also recommends that there be separate information-sharing protocols for operational and regulatory information. While there will naturally be overlap between the two in terms of the content of the information, our suggestion is based on the primary purpose for providing information. Specifically, our recommendation is that if information is provided to an agency for operational purposes, it can only be used by that agency. However, if information is provided to a regulator, it could potentially be shared with other regulators (under appropriate protocols) for the purposes of investigating an incident.

12. This separation would support the government's objective of better supporting critical infrastructure entities to manage cyber incidents by improving both the efficacy of an entity's response and the clarity of the information it provides. It would also incentivise industry to be more forthcoming with cyber incident information, a key concern of government noted in the consultation paper. One of the key reasons that some entities might be hesitant to provide information is a lack of certainty about how it might be used and by whom. By creating a secure, contained avenue for the sharing of operational information, entities can have more confidence that this information will only be used to support the incident response itself. This of course would not exempt entities from any reporting requirements to regulatory bodies or the need to provide full and frank information to an inquiry. Rather it would allow them to separate the two processes, leading to a more effective incident response, followed by clearer information being provided to regulators once the incident itself had been managed.

## DEFINITIONS AND THRESHOLDS NEED FURTHER CLARITY

13. There are a number of definitions and thresholds in the consultation paper that would benefit from further clarification. These include:

    (a) The parameters of information-sharing under the limited use obligation;

    (b) The threshold for invoking the consequence management powers;

    (c) The meanings of 'business critical data' and 'material risk' under the proposed data storage and processing amendments; and

    (d) The meaning of 'seriously deficient' under the proposed review and remedy powers.

***Limited Use Obligation***

14. Optus supports the intention behind the proposed limited use obligation (Measure Three) but encourages the government to go further by clarifying and strengthening the limits on information-sharing between agencies. Building on our suggestion in the previous section, an important basis for entities having confidence in providing information is not incurring unintended legal liability by doing so. While entities should of course be accountable for meeting their regulatory obligations, the information shared in the early stages of an incident may not always be complete. This incomplete information can later be taken out of context or otherwise misrepresented, despite it reflecting the best available knowledge of the affected entity at the time it was provided.

15. This possibility disincentivises the sharing of information with government agencies, especially when, as is the case under the proposed limited use obligation, there is a clear intent to be able to share information with other agencies, including regulators. Addressing this situation – through the separation proposed in the previous section – would alleviate this concern and encourage better information-sharing from critical infrastructure entities. This would improve incident response processes while also bolstering government's awareness of the national cyber threat picture, a key goal of the Cyber Security Strategy 2030.

***Consequence Management Powers***

16. While the consultation paper includes several criteria for invoking the consequence management powers (Measure Six), it is not clear that a non-cyber incident could ever reach these thresholds. The government already has similar step-in powers for cyber incidents under Part 3A of the SOCI Act so it would seem that government is seeking to expand these powers to incorporate all potential hazards.

17. However, Optus notes that the existing step-in powers are yet to be invoked for any of the cyber incidents that have occurred since these powers were legislated in 2020. Moreover, it is not clear that a non-cyber incident could ever reach the threshold required for such powers to even be contemplated. The Act requires that an incident threaten the socio-economic stability, national security or defence of Australia. In addition, it requires all other regulatory avenues to be exhausted first and for the entity to be unwilling or unable to address the incident. No incident to date appears to have come close to meeting even one of these thresholds let alone all three.

18. It is difficult to foresee when these powers might be capable of being invoked and therefore it would be beneficial if further work was done to demonstrate their necessity.

***Data Storage and Processing***

19. Two of the key definitions under the proposed data storage and processing amendments would benefit from clarification: 'business critical data' and 'material risk'.

20. It is worth noting that a critical infrastructure entity's default definition of 'business critical data' will differ from that of the government. Whilst critical infrastructure entities understand the broader importance of their obligations, they are commercial organisations and their perspective of 'business critical' will include a number of commercial considerations, whereas government's may not. It is therefore important that government, when developing the relevant amendments, consult further with industry to develop a clear, practical definition of 'business critical data'.

21. Similarly, critical infrastructure entities would benefit from further guidance on what is considered to be a 'material risk' to this data. Again, there may be a variation in what critical infrastructure entities include in their risk matrices compared to government. Clarifying the risks that government expects entities to consider would help improve their capacity to comply with the new obligations.

## FURTHER WORK IS NEEDED ON TWO PROPOSALS

22. Two of the government's proposals – the Cyber Incident Review Board and the consequence management powers – would benefit from further work to demonstrate the need and utility of the proposals. Both of these proposals raise a number of concerns, particularly around the use of sensitive information and the significant expansion of emergency powers.

23. While Optus strongly supports better sharing of government threat information and lessons learnt from cyber incidents, it is not clear that a separate function needs to be established for this purpose. The Australian Cyber Security Centre (ACSC) already gathers information from industry and provides regular guidance on responding to the latest vulnerabilities. If government's view is that this existing process is insufficient, Optus suggests that it would be more effective to make the necessary changes to this existing process rather than establishing a new one.

24. In addition, the proposal for a standalone Cyber Incident Review Board raises several concerns about the appropriate handling of sensitive information. Given the Board would be examining cyber incidents, it would necessarily have access to very sensitive information about the network of critical infrastructure entities. It is not clear what information and personnel security measures would apply to Board members to ensure the appropriate protection of this information.

## MEASURE 1 – SECURE-BY-DESIGN STANDARDS

25. Optus supports the government's intention to regulate secure-by-design standards for smart and internet of things devices. To improve the efficacy of these proposals, we offer the following comments based on our experience:

(a) Primary responsibility for adhering to these regulations should sit with manufacturers and importers. Manufacturers for such devices are almost entirely overseas and importers will be the first point of entry into the Australian market for these devices.

(b) There are several practical considerations that government needs to consider when designing these regulations:

(i) First, one of the most common vulnerabilities in smart devices is at the account holder level, not the device itself. For example, a common occurrence in domestic and family violence cases is for someone to create a duplicate account. This duplicate is then covertly maintained to harass and/or conduct surveillance. This vulnerability would not be addressed under the proposed regulations.

(ii) Second, the list of regulated devices should be risk-based in terms of the information the device is capable of transmitting or storing. Many smart appliances – such as washing machines or ovens – are unlikely to transmit or store any sensitive information, they simply receive prompts or run automation processes. On the other hand, devices such as video doorbells can record and store both video and audio, giving them a much higher risk profile.

(iii) Third, it is not clear how compliance with the regulations would be assured. One possibility could be for a labelling system to be introduced, indicating that a device complies with the relevant standard. For the telecommunications industry specifically, there is already an independent test lab system that reviews network hardware for security vulnerabilities and standards compliance. It would be worth government clarifying whether they are considering an expansion of this system and, if so, how they envisage it might work.

(iv) Finally, there are a number of existing Australian regulations and standards for some smart devices, particularly security products. Government should ensure that any proposed regulations align with these existing frameworks.

**Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?**

- As noted above, primary responsibility should rest with manufacturers and importers.

**Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?**

- Optus supports these principles as the basis for the proposed regulations.

**What types of smart devices should not be covered by a mandatory cyber security standard?**

- Optus does not support the inclusion of smart phones in the proposed regulations. There are already many global and Australian regulatory obligations applicable to smart phones sold in Australia and therefore it would be duplicative to implement an additional regime for such devices.

**What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?**

- A minimum of twelve months would be an appropriate timeframe.

## MEASURE 2 – RANSOMWARE REPORTING

26. As noted in our original submission on the cyber security strategy, Optus recommends that the government harmonise the various reporting requirements into a single framework that eliminates duplication. This would improve the capacity of critical infrastructure entities to focus on incident response as well as streamlining information flows for government agencies.

27. Optus also reiterates its position on ransomware payments: it would be highly beneficial to have a strong message for criminals that ransoms will not be paid through a mandatory prohibition. With such an approach limited exceptions might nonetheless be required to be applied on a case-by-case basis.

**What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?**

- Optus supports the proposed 72 hour period as an initial notification requirement, noting the possibility that little concrete information would be available at such an early stage.

**To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident to Government?**

- Refer to the relevant section in the body of our submission.

**How can the Government ensure that the no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?**

- Refer to the relevant section in the body of our submission.

## MEASURE 3 – LIMITED USE OBLIGATION

- Refer to the relevant section in the body of our submission.

## MEASURE 4 – CYBER INCIDENT REVIEW BOARD

- Refer to the relevant section in the body of our submission.

## MEASURE 5 – DATA STORAGE AND PROCESSING

- Refer to the relevant section in the body of our submission.

## MEASURE 6 – CONSEQUENCE MANAGEMENT POWERS

- Refer to the relevant section in the body of our submission.

## MEASURE 7 – PROTECTED INFORMATION PROVISIONS

28. In line with our comments about the limited use obligation, Optus suggests that more clarity is needed about the ability of third parties to access protected information in the wake of an incident (e.g. through FOI requests). While Optus supports the need to disclose sensitive information for regulatory, security and other legitimate purposes, it would be concerning if third parties could access protected information without a legitimate basis for doing so.

## MEASURE 8 – REVIEW AND REMEDY POWERS

29. Given the strong relationship between this measure and Measure 9 for the telecommunications sector, Optus suggests that it is best dealt with through the ongoing work of the Australian Telecommunications Sector Reference Group.

## MEASURE 9 – CONSOLIDATING TELECOMMUNICATIONS SECURITY REQUIREMENTS

- Optus is currently working through the co-design of this measure as part of the Australian Telecommunications Security Reference Group (ATSRG).

**[End of Submission]**