OPTUS

Submission to the
Department of Home Affairs

Response to Government Discussion Paper: Cyber Security Strategy

Public Version

April 2022

EXECUTIVE SUMMARY

1. Optus welcomes the opportunity to provide a submission on the Government's Cyber Security Strategy discussion 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. 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. Optus strongly supports the government's ambition for Australia to be the most cyber secure country by 2030. Based on our experience, we offer the following key comments for consideration:

    (a) The overarching goal of the cyber security strategy should be **improved cyber resilience**; and

    (b) Government should **establish permanent crisis response arrangements with industry**, overseen by the National Cyber Coordinator and drawing on the experience of recent cyber incidents. Key elements would include:

        (i) **Flexible standing arrangements**, similar to those that exist in Home Affairs and the Department of Foreign Affairs and Trade (DFAT).

        (ii) **Streamlined reporting requirements** that minimise duplication and prioritise operational and law enforcement responses.

        (iii) **Safe harbour protocols** that allow for full and frank information-sharing without this being this being prejudicial in future regulatory investigations or legal actions.

5. In addition to these overarching suggestions, we have offered more specific responses to a number of the questions in the discussion paper. We would welcome the opportunity to discuss any of these issues in further detail.

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

Resilience Should Be the Overarching Goal

7. Previous cyber security strategies have tended to focus on operational or short-term policy actions that, while beneficial, may not have provided the best foundation for long-term improvements. Setting an underlying goal of being the most cyber secure nation in the world by 2030 represents a welcome step-change in the approach and will help both government and industry achieve a significant, long-term uplift in cyber security capabilities and outcomes.

8. Optus also supports the government's goal of ensuring that the regulatory system provides the appropriate balance between consumer protection and innovation and growth. Technological innovation is a crucial ingredient in improving cyber security capabilities. It is vital that our policy settings enable this to the maximum extent possible whilst retaining the appropriate protections.

9. Cyber attacks are an unfortunate reality of modern life and will continue to occur. While every effort should be made to minimise the chances of a breach from such attacks, the fact is that resilience in the face of breaches is also very important. Improved resilience will create a virtuous cycle whereby Australia becomes an increasingly less attractive target for malicious actors. The better we can withstand attacks and the faster we can recover, the less there is to be gained in the first place.

10. One way to do this is to devalue the personal information to a criminal by redesigning systems to assume much of the relevant information is out there already and to introduce digital identity documents in conjunction with more secure technologies, like biometrics. By reducing both the amount and nature of personal information held by companies, the value of illegally accessing such information through criminal attacks is diminished. Optus notes that the Australian Government is starting to take steps in this regard, including working with the NSW Government to explore the use of digital identity documents on the MyGov platform.

11. Optus has also undertaken a similar initiative by partnering with Mastercard to develop a digital identity process. This allows people to create a secure and reusable digital identity profile that removes the need for customers to use (and service providers to store) copies of physical identity documents. Initiatives like this which reduce the information held by companies reduce the customer information that can be compromised and exposed to fraud risk in the event of data theft.

12. We would encourage the government to continue these efforts and would welcome the opportunity to discuss our own experience in further detail.

Government Should Establish Permanent Crisis Response Arrangements with Industry

13. A key lesson of Optus's cyber incident was the criticality of effective cooperation with government. Optus had to engage with over 20 federal and state/territory agencies on a range of issues from law enforcement and regulatory investigations, through to identity document replacement processes, as well as the operational response itself.

14. Optus worked with the federal government on the establishment of a Working Group with senior executives from Home Affairs, Prime Minister and Cabinet, DFAT and Services Australia to streamline the coordination of information and response. This group provided welcome coordination across the range of policy challenges posed by a major cyber incident, including consistent information flows across decision-makers in the public service, ministers and their offices.

15. The Working Group also provided a critical forum for Optus to provide regular updates and advice to government as well as to receive clear guidance from government on the various policy considerations involved in managing the response.

16. Given the efficacy of the Working Group, Optus recommends that such a model could form the basis of permanent crisis response arrangements for serious cyber incidents. These arrangements could be overseen by the forthcoming National Cyber Coordinator and should be flexible and adapt to the particular circumstances of an incident.

    (a) For example, if an incident involves a state actor, it may be the case that technical assistance is the most valuable support that government can offer. Alternatively, if an entity is capable of responding to an incident at an operational level but needs to coordinate with numerous government agencies as was the case with the Optus incident, policy agencies would be better suited to lead the government response. In any event, both technical and policy agencies should always be involved to ensure consistency and effective coordination.

    (b) If there are many identity document licensing authorities involved, the Working Group could ensure a consistent approach among federal departments for the replacement of government identity documents and this could also be extended to include state departments.

17. These arrangements could also consider ways to co-ordinate the regulatory responses to an incident, including by acting as a single reporting source for the affected entity. In particular, establishing mechanisms that prioritise operational and law enforcement responses would assist both government and entities affected by a major cyber incident to focus their resources on the initial and most urgent response efforts. This point is discussed in more detail in the next section.

18. Finally, the Australian Cyber Security Centre and Australian Federal Police have emphasised to Optus how much they value fast, transparent action and how powerful it can be in helping everyone work together effectively. To support this further, the Australian Government may wish to consider how these crisis arrangements could incorporate safe harbour protocols. These protocols would encourage the full, frank and early sharing of information (before it has been fully verified) without this being prejudicial in future regulatory investigations or legal action.

19. We would welcome the opportunity to discuss these and our discussion paper responses in more detail. Our responses to the specific discussion paper questions begin over the page.

DISCUSSION PAPER QUESTIONS

Legal/Regulatory

What legislative or regulatory reforms should the government pursue to enhance cyber resilience across the digital economy?

See questions below.

Government

What can the government do to improve information-sharing with industry on cyber threats?

- Look at ways to continue enabling better strategic intelligence-sharing to inform cyber defences. The present focus is on sharing operational information after a vulnerability has been identified/breach has occurred. There would be significant benefits in sharing broader information that may assist in preventing vulnerabilities from being exploited in the first place.

- We appreciate that the Australian Cyber Security Centre (ACSC) has established the Cyber Threat Intelligence Sharing (CTIS) programme and would encourage the Government to be ambitious in its scope and implementation.

What more can the Australian Government do to support Australia's cyber security workforce through education, immigration and accreditation?

- One area for greater flexibility is the strict requirement that any security clearance holder must be an Australian citizen. Whilst there will of course be a need to retain this requirement at higher levels, other countries, including Five Eyes partners such as the UK, operate a limited clearance process for citizens of trusted partner countries. This could broaden the trusted skills base within the cyber security eco-system.

How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

- Often there is benefit in coordinated public messaging to ensure consistent advice, reassure affected citizens and provide a clear pathway out of the incident. Government could consider ways to incorporate the affected entity/ies into its crisis response arrangements (as appropriate) to coordinate on messaging and mitigations. The aim of such an approach would be to provide appropriate risk-based transparency.

- The Australian Cyber Security Centre and the Australian Federal Police have both emphasised to Optus how much they value fast transparent action and how powerful it can be in helping everyone work together effectively. To support this approach, the Government may wish to consider developing safe harbour protocols that would encourage the full and frank sharing of information with key government agencies early and often before this has been fully verified without this being prejudicial in any future regulatory investigations or legal action.

How can government and industry work to improve cyber security best practice knowledge and behaviours and support victims of cyber crime?

- Government should consider itself the primary party responsible for protecting citizens from crimes.
- Government could consider a system of rating the impact to individuals of a cyber incident to help inform overall response.
    - For example, depending upon their particular circumstances, customers will be impacted in different ways by a cyber incident. This nuance is difficult to communicate in a crisis, however, so having some form of independent impact-rating system operated by government could be a useful communications and crisis management tool. Such a system would not only help triage the actual crisis response but also help reassure people in general during a serious incident, reducing community uncertainty.
- This should be done by government or a qualified neutral party so companies are not limited by their own field of vision.
    - For example, identity theft could occur via a hotel chain but the key risk may manifest as compromised bank details that result in money being stolen and implications for a financial institution. There is no way to be sure that executives of a hotel company can predict the implications of how data is used outside their industry and so their responses may be insufficient to protect customers.

What opportunities are available for government to enhance Australia's domestic cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

- Government could provide more transparency through Telecommunications Sector Security Reforms (TSSR) on vendors who are 'not high risk' and streamline the process for telecommunications providers to understand this. For example, maintaining a centralised understanding of vendors who have already been subject to TSSR review and deemed not high risk and streamlining the procurement process for these vendors.

How should we approach cyber security technologies future-proofing out to 2030?

- Traditional methods of protection and regulation may not be well-suited to modern threats and can hinder innovation. Government should consider ways to encourage innovation in cyber security technology, allowing us to keep pace with the threat landscape. This could include expanding trusted digital identity frameworks (as is being done with MyGov and NSW Government's digital ID app), stronger encouragement of two-factor/multi-factor authentication, review of the hundred-point check model, mechanisms for decentralised data storage and promotion of data classification and data loss prevention technologies.

Are there opportunities for government to better use procurement as a lever to support the Australian cyber security technologies ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

See response to question above regarding the domestic cyber security technology ecosystem.

How should the Strategy evolve to address the cyber security of emerging technologies and promote security-by-design in new technologies?

See response to question above regarding cyber security technology future-proofing.

Consolidated Regulatory Questions

What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

- Fostering innovation needs to have greater prominence in the strategy as this will generate the technological solutions to help combat rapidly evolving threats.

- An innovation mindset also needs to be applied to regulatory design, in that a greater emphasis on principles-based and outcomes-based regulations should be adopted. Prescriptive requirements will always fail to keep pace with evolving threats and technology, while also imposing costs on industry and hindering innovation.

What legislative or regulatory reforms should government pursue to: enhance cyber resilience across the digital economy?

Note: we have only included questions for which we have provided a response.

- What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation or further regulatory guidance)?

    a. *A greater emphasis should be placed on clearer and more comprehensive guidance. The United Kingdom is an example of a jurisdiction that takes this approach and it provides an ideal balance between clarity for industry and greater compliance for government as a result.*

- Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

    a. *It is not evident that customer data and 'systems' would reach the high threshold of the Act, i.e. an asset/system that, if significantly compromised, could jeopardise national security, economic stability and the national interest). Expanding the definition of a critical asset also risks diluting the resources that can be directed towards the protection of critical assets as currently defined.*

    b. *It would be worth giving more time for the SOCI laws and regulations to mature, using the current definition of critical assets, particularly when some elements are still yet to be enacted. This would allow time to assess the impact of the legislation and build an evidence base as to whether/where further reform might be needed.*

    c. *Moreover, the review of the Privacy Act has a significant focus on the protection of personal and sensitive information. It would be prudent to allow this review and the forthcoming legislative changes to be implemented before consideration is given to regulating personal information under another Act.*

- Should Australia consider a Cyber Security Act and what should this include?

    a. *This could be beneficial if it consolidates in one place all existing legislation that deals with cyber. Otherwise, it is difficult to see what a Cyber Security Act would entail given there is already a broad range of legislation that regulates cyber security risks in various ways, including the Security of Critical Infrastructure Act, Privacy Act and, in the case of Optus, the Telecommunications Act.*

    b. *It is also hard to reconcile one of the key goals of the strategy – harmonising regulatory architecture – with the creation of an entirely new piece of legislation.*

- Should the government prohibit the payment of ransoms and extortion demands by cyber criminals by:

    a. Victims of cybercrime; and/or

    b. Insurers?

    c. If so, under what circumstances?

        i. *Optus suggests that 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 be required to be applied on a case-by-case basis in collaboration with government.*

- Should government clarify its position with respect to payment or non-payment of ransoms by companies and the circumstances in which this may constitute a breach of Australian law?

    a. *See above*

- What can government do to improve information-sharing with industry on cyber threats?

    a. *Given the seven-year outlook of the strategy, there would be value in looking at how government might establish the infrastructure for better sharing of classified threat information with industry. While there can be challenges with granting industry personnel appropriate security clearances, the larger challenge is building the IT infrastructure to enable the actual information-sharing that would be of most use to industry.*

    b. *Government is already focused on hardening its own IT infrastructure through this strategy so there may be a natural synergy with that process and exploring ways to incorporate industry. Five Eyes partners such as the United States and United Kingdom operate fusion centres that could serve as a useful model.*

- During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) and ACSC improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

    a. *As noted earlier, Optus sees significant value in having appropriate safe harbour provisions to allow for full and frank information exchanges with operational agencies. This is crucial for enabling the most effective operational response possible without this being prejudicial in possible regulatory investigations or legal actions.*

    b. *We should note that this obligation should also apply to the National Coordinator and any other departments brought into the immediate response as they too will need full access to information.*

- How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

    a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

        i. *Yes, but this should be part of a broader consideration of effective incident management arrangements with industry. See the main body of our submission for a more detailed discussion.*

ii. *Such a portal would by definition be exposing methods of attack, vulnerabilities, etc and should therefore be subject to the highest security protection standards.*

- What would an effective post-incident review and consequence management model with industry involve?

    a. *As outlined in the body of our submission, government should consider establishing permanent but flexible crisis response arrangements and be very careful with any consequence management frameworks.*

[End of Submission]