Protecting Critical Infrastructure and Systems of National Significance

Consultation Questions

1. Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Yes Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)? No

2. Do you think the current definition of Critical Infrastructure is still fit for purpose? Yes

3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?

   PBPL does not influence other supply chain entities eg Stevedores who are maritime security plan holders in their own right

   Other factors include Supply chain links (components in manufacturing chain) – chips into motherboards into PC's (unseen dependencies)

4. What are the common threats you routinely prepare for and those you have faced/experienced as a business?

   Detailed in Port Wide Risk Assessment submitted to AMS as part of approved Maritime Security Plan.

   Cyber security is currently our own initiative, outside the realm of the Port Maritime security plan, and will need to be mapped to future legislation

5. How should criticality be assessed to ensure the most important entities are covered by the framework?

   The scale of dependency eg how many other business rely on the entity and also the impact to other industries if they are disrupted, eg do they provide a fundamental service such as power?

6. Which entities would you expect to be owners and operators of systems of national significance?

   As identified under the Security of Critical Infrastructure (SOCI) legislation

7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?

   It would allow wider participation in TISN and more proactive communication from TISN

8. What might this new TISN model look like, and what entities should be included?

   As identified via SOCI legislation

9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?

   A risk identification and analysis framework with a set of questions or tools to be used to identify and rank risk. Also, the provision of audit consultation teams within government to assist with identification.

10. Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with? Yes

11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

    This is difficult to comment on given the strategy and consultation paper are still at high level

12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

    Some of the principles in PSO are already being broadly adhered to, however, depending on the details of how this is going to be regulated there may be additional time and costs incurred.

    The Enhanced Cyber Security Obligations are of more concern depending on the details of what this obligation is going to entail. This could take significant time and costs to achieve. The compliance with ASD Essential 8 level 3 for MSIC operations took 12 months and initially significant cost with ongoing OPEX costs being incurred for the secure environment as well as annual audit and compliance obligations. These additional costs will need to be recovered from all user of Infrastructure facilities.

13. What costs would organisations take on to meet these new obligations?

    All additional costs for compliance, passed onto beneficiary / user of port services.

14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

    In Port environment recent upgrades to MSIC security systems have been implemented, noting question 12 re cost implications. Port Operators such as Stevedores and Fuel operators also hold security plans and may be affected by CIC changes. We now await review of upcoming legislation to assess obligations.

15. Would the proposed regulatory model avoid duplication with existing oversight requirements?

    These need to blend with AMS port security regulations and legislation

16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?

    Ensure they include proposed cyber security arrangements

17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

    Limitation is most likely the cyber part of the obligations – must be a federal regulated entity rather than state based.

18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

    Cyber Audit training and broader industry understanding will be essential as they will be paying for this work. It will require realistic expectations of the regulations and what is going to be audited. It also needs realistic timing expectation of when this will be implemented

19. How can Government better support critical infrastructure entities in managing their security risks?

    More information sharing, regularly updates on best practice, provision of list of certified vendors or products, information on organizations / suppliers which breach national security interests

20. In the AusCheck scheme, potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?

    Extend the requirement for MSIC and security checks to all maritime employees, and not just those that work on the waterside zones. Insider threat is considered high risk now.

    There may need to be other background checks for IT personal working in critical infrastructure cyber security and also support staff working on Critical Systems within entities. Additional costs associated with increased security clearances will be passed on by PBPL to end users / customers and we anticipate any vendors required to comply with this will also pass on costs.

21. Do you have any other comments you would like to make regarding the PSO?

    How do the PSO relate to outsourcing arrangements entities might have?

22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

Listing systems or software which are critical to the infrastructure entity, eg what components are critical to keep the business operating.

Government may need to define their cloud usage policy / overseas data storage policy for CIC entities (eg are there going to be directions on which cloud providers we can use / where we are able to store our data) so that we can evaluate impact of these type of directives.

23. What information would you like to see shared with critical infrastructure by Government? What benefits would you expect from greater sharing?

    More timely information on emerging threats, trends seen elsewhere to enable us to take more timely preventive steps – eg early blacklisting / preventative patching. This is one reason why it would be important to increase the membership of TISN.

24. What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?

    PBPL is currently not able to assist however we may be able to in the future, once we have implemented more automated continuous threat detection software – TISN would be important. The costs cannot be identified until the mechanism of contribution is defined.

25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

    The meaning of this question is unclear as we have a number of network perimeters – including third party interactions with telco providers for example.

    It would be useful to have a government perimeter which was protecting all CIC entities.

26. What are the barriers to owners and operators acting on information alerts from Government?

    Understanding the relevance of the threat to our environments – having the tools to do the same level of analysis which government is able to re detection of any penetration of the threat into our environment (this will be partly addressed with implementation of new continuous threat detection software)

27. What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?

    Playbooks will need to consider the different level of maturity and sophistication of tools available to each entity. Playbooks need to consider entities within a CiC node eg stevedores at Ports as an example.

28. What safeguards or assurances would you expect to see for information provided to Government?

    PBPL would expect the same levels of information security which we provide over our own data based on the data classifications eg encryption at rest; SFTP transmission, etc

29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

    For discussion as part of the preparation of scenarios and playbooks.

30. Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?

    Government, as an example selected committee by majority vote including Minister, Cyber Security head and legal representative, and to include advice from the impacted entities

31. Who should oversee the Government's use of these powers?

    Independent Ombudsman – not the minister

32. If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber-attack, do you think there should be different actions for attackers depending on their location?

    Credible scenarios need to be contemplated as part of the playbook process to respond in case of cyber-attack considering supply chain implications in the scenarios

33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?

    Appropriate indemnities against cost claims from other entities disrupted when taking emergency actions,

34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these types of powers?

    Independent body to provide oversight on decisions.

35. What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?

    The risks include Trade and supply chain implications and disruptions. The costs will depend on what is regulated and will be passed onto end users / customers.

36. Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?

    Private entities will retain the right to recover costs from beneficiaries – end users / customers.