Australia Post

Submission

Protecting Critical Infrastructure and Systems of National Significance

16 September 2020

auspost.com.au

Classification: Public

Executive Summary

Australia Post welcomes the opportunity to provide a submission input to the Department of Home Affairs relating to the consultation paper on Protecting Critical Infrastructure and Systems of National Significance.

The threat landscape is rapidly changing and evolving, and it has never been more important to ensure that Australia's most critical assets are protected and resilient against these threats.

With this initiative comes an opportunity to introduce an enhanced regulatory framework that will be consistently applied across all critical infrastructure sectors, driving resilience and protecting our most Critical Infrastructure and Systems of National Significance.

Australia Post supports a principles-based approach to enhancing the regulatory framework, however there is an opportunity to be specific about risk management best practices, cyber security controls and reporting frameworks. A consistent, standards-based approach could aid in adoption of the enhanced framework, and also the regulators ability to govern an organisations compliance.

Below, Australia Post has provided responses to the majority of questions outlined in the consultation paper. Where Australia Post has no specific comments or response to particular questions at this time, this is indicated.

Responses to Consultation Paper Questions

1. Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?

   The sectors listed broadly cover and capture the vital industries for Australia. Consideration could also be given to how Government entities fit into these proposed reforms.

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

   There is an opportunity to review the current definition to ensure that all of the relevant infrastructure assets are included. Under the current *Security of Critical Infrastructure Act 2018*, the assets defined as critical are:

   (a) a critical electricity asset; or
   (b) a critical port; or
   (c) a critical water asset; or
   (d) a critical gas asset; or
   (e) an asset declared under section 51 to be a critical infrastructure asset; or
   (f) an asset prescribed by the rules for the purposes of this paragraph.

   Consideration could be given to the other sectors outlined in the consultation paper to determine the criticality of each, and the impact on our society, economy, security and sovereignty if the essential services these assets provide become unavailable.

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?

   No specific comments or response to this question at this time.

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

   Broadly we prepare for business disruption using an all hazards approach. From a cyber security perspective, we routinely prepare for threats that can have an impact on the confidentiality of, availability or integrity to, Australia Post systems or information. We continue to experience and defend against various threats types including Unauthorised Access, Malware, Denial of Service and Information Disclosure.

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

   Over and above the currently defined critical entities and assets, the following could be considered when assessing criticality:

- likely economic impact – financial, employment, etc;
- availability of basic human essentials (ie medical, food & grocery; transport – delivery of basic essentials; banking);
- market share of critical systems or services;
- dependencies (supply chain);
- size of business;
- community impacts; and
- entities' national exposure and presence.

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

Energy / Gas; Water; Ports – Air and Sea; Major Telecommunications; Cloud and Data; Defence; and Health.

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

A revised TISN could drive greater collaboration across all parties and provide a trusted forum where information can be shared openly. Recognition and understanding of other essential entities that either stand alone or support critical infrastructure would also be useful.

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

Consideration for an overarching TISN in addition to industry specific sub groups. Alternatively, consideration could be given to sub groups based on a criticality class. From a cyber security perspective, Australia Post considers the Australia Cyber Security Centre National Information Exchange a good example, where information is shared openly between government and industry.

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?

Joint seminars and discussion exercises to better understand requirements, impacts and reliance on each other. Joint simulation exercises focusing on realistic threats, leading to a better understand of requirements, impacts and entities and Governments reliance on each other.

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

The principles or principle-based outcomes do appear sufficiently broad to cover all aspects of risk across sectors. The principles being: Identify and understand risks; Mitigate risks to prevent incidents; Minimise the impact of realised incidents; and Effective governance.

Consideration could be given to applying more consistency with how entities define and understand risks. A single risk management framework may limit subjectiveness (type, value and security objectives for the systems) across sectors with differing risk management maturity. The risk management framework used by the Australian Government Information Security Manual is a potential framework (ie define the system, select security controls, implement security controls, assess security controls, authorise the system and monitor the system).

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

The security requirements, or obligations, cover the high-level areas for providing effective security coverage. The requirements here are broad and non-specific at this stage. Within the Cyber security section, terminology such proportionate controls, best practice guidelines and robust security measures are used. This terminology is non-specific which can lead to confusion as to what to implement and how to measure effectiveness. The opportunity exists to be specific so that entities know what they need to implement from both a framework and controls perspective.

Positive Security Obligation (PSO) can also be more prescriptive with control expectations (though understanding this is principles based), for example: Mitigate risks to prevent incidents – providing a controls framework may assist with risk mitigation, including supply chain risk. Clarifying the expectations for robust security measures may involve suggested security controls for the systems to achieve desired security objectives.

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?

The requirements in the consultation paper are currently principles based and non-specific. Entities could indicate that they are operating in-line with these principles, within their own context. Without understanding if there is to be a prescriptive framework and/or set of controls to be implemented, it is not possible to understand time and/or financial impact to meet these principles.

If organisations are legally obliged to manage risks that may impact business continuity and Australia's economy, security and sovereignty, by meeting the PSO principles-based outcomes there will be both time and cost implications. Specifically:

- once suitable security controls have been identified and agreed upon for a system, they could be implemented;
- monitoring systems, and associated cyber threats, security risks and security controls, on an ongoing basis;
- a clear definition of in scope assets will also drive time and cost for an organisation; and
- assume an uplift in cost to monitor and report compliance against framework. Further detail would be required to be specific on the significance of this cost increase.

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

Organisations will generally already have prioritised business, technology and cyber security programs of work. These new obligations would need to be factored into the prioritisation of this existing work, funding availability and priorities.

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?

No specific comments or response to this question at this time.

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

Until a further level of detail and clarity is developed on any new obligations, it is difficult to determine if duplication will be avoided. As further detail is worked through to determine which frameworks, controls and reporting obligations each sector needs to adhere to, it is highly possible that this model could supersede or replace existing models.

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?

The sector regulator could provide frameworks, advice, information, reporting timelines, templates, online publications etc, to support organisations in meeting the PSO. This could include websites; online seminars; workshops

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?

No specific comments or response to this question at this time.

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

Government advisors, support networks between each sector and a clear framework for them to follow and understand their obligations as regulators.

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

Clear, simple guidance with reporting templates that are easy to use and complete.

Potential for automated reporting for organisations with agreed format and how risks should be managed (ie mitigation strategies, issues identified, timing, etc)

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?

No specific comments or response to this question at this time.

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

Consideration for leveraging existing industry or government frameworks could be given. This would assist organisations in meeting their PSO obligations and would limit any 'new' requirements which may be costly and difficult to meet. Risk mitigations should arguably be balanced with each organisation's risk appetite.

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

There are many preparatory activities that should be part of an entity's cyber security program, including, but not limited to:

- regularly vulnerability scanning and patching in alignment with best practice;
- application and system hardening;
- regular cyber simulations and tests;
- incident runbooks;
- regular education and awareness sessions for employees;
- following best practices such as least privileged access to critical systems and data;
- regular testing of backup and recovery plans; and
- segmentation of critical systems to limit and/or contain issues when/if they arise.

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

By making available, or increasing access to real-time reporting of critical issues, emerging threats and/or availability of Indicators of Compromise (IOCs), entities will have the ability to be on the front foot of pending attacks. This type of information sharing, even by sector, can be vitally important in helping entities respond quickly and ensure the appropriate protections or mitigations are in place.

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?

We could contribute information such as Techniques Tactics Procedures (TTPs) or IOCs relevant to threat sightings across our environments. In addition, we could provide intelligence relating to threats that we have observed. We anticipate costing to be negligible on the basis that we can integrate with a Threat Intelligent Platform via standard patterns.

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

There are many methods to identify vulnerabilities at a perimeter level. Common methods could include:

- using a web, system, application vulnerability scanning tools to passively scan for known issues;
- using port scanning techniques to ensure only secure network ports are open and exposed to public networks;
- penetration testing;
- continuous vulnerability scanning;
- social engineering exercises;
- red / purple team exercises; and
- underground forum / dark web monitoring.

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

There are many capabilities that an entity must have to act on alerts, including, but not limited to the following:

- understanding the applicability of any such alert and its relevance to the entity's context or environment:
- understanding of how to apply any mitigations or fixes to nullify or remove the risk caused by such an alert;
- appropriately skilled personnel to interpret the alert and apply any fix or mitigation; and
- where an alert requires investment to correct or mitigate, the financial means and/or priority to respond and implement.

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

A standard set of playbooks would be greatly help entities understand what they need to develop and test. We foresee no known barriers for playbook co-development. Suggested information to be included is below.

- roles and responsibilities;
- engagement points and contact information;
- rules of engagement;
- incident priority rating table;
- response steps (eg containment, eradication, recovery);
- reporting matrix / communications plan;
- business continuity planning (at a government level); and
- alignment and understanding of an entities' existing processes (ie crisis management).

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

Appropriate confidentiality, handling and storage of information collected from organisation as part of independent assessments by third-party providers; light-touch vulnerability scanning and assessment to identify vulnerabilities at the perimeter of critical networks.

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

As identified in the consultation paper, where government identifies an immediate and serious cyber threat to Australia's economy, security or sovereignty (including threat to life). In these situations, it may be appropriate for government to declare an emergency. Permissible actions could include allowing government to assist entities take technical action to defend and protect their networks and systems, and provide advice on mitigating damage, restoring services and remediation.

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?

No specific comments or response to this question at this time.

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

No specific comments or response to this question at this time.

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?

If there is an ability to block or stop an international based attack on Australian entities, disruption of such an attack at a geolocation level or a telecommunications level would be welcomed. Many organisations do not have the scale, compute power, or bandwidth to block or stop large scale Nation State-like attacks. There is potential for a difference in response based on the context of the attack and the potential capabilities of the suspected actor. Different response actions for attackers based on location could be problematic. Ensuring an attacker is in fact from a certain location can be difficult. A standard response no matter the location could be a simpler approach.

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

No specific comments or response to this question at this time.

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

No specific comments or response to this question at this time.

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?

No specific comments or response to this question at this time.

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?

No specific comments or response to this question at this time.