Office of Chief Safety & Risk

GPO Box 367

Canberra

t 02 6268 5170 **www.airservicesaustralia.com**

ABN 59 698 720 886

Critical Infrastructure Centre | Department of Home Affairs

1300 27 25 24 | ci.reforms@homeaffairs.gov.au

As Airservices' appointed Chief Security Officer, I am writing to provide feedback on the recently released *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper, August 2020.*

Our detailed response is contained at **Attachment 1**. In summary, we agree with the principles and risk based approach to the protection of Critical Infrastructure. Airservices Australia looks forward to participating in an enhanced Trusted Information Sharing Network (TISN) that includes the broader elements of protective security, supply chain and asset risk management. We welcome the opportunity to provide input and support to government in protecting the essential Air Traffic Management and Aviation & Rescue Fire Fighting services and associated critical infrastructure that Airservices manages across the Australian airspace.

If you require any further information, please contact Tracey Lawrance, Governance & Security Manager ([redacted] or Silas Barnes, Chief Information Security Officer ([redacted]).

[redacted]

Claire Marrison

Chief Safety & Risk Officer

16 September 2020

Attachment 1

Protecting Critical Infrastructure and Systems of National Significance

Airservices Australia Response

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)?	Aviation needs to be better articulated under the Transport Sector. Includes Airports, Airlines, Air Traffic Management (ATM), and airspace management (Airservices Australia). The changing risk context of the aviation environment including Unmanned aircraft system Traffic Management (UTM) and space-based surveillance could present new threats to the National security environment. The UTM concept incorporates System Wide Information Management (SWIM), Artificial Intelligence (AI), Geo-fencing and advanced telecommunication networks to safely and efficiently integrate UTM with existing flying operations. Whilst the focus is on cybersecurity, we see an opportunity to consider hazards associated with positioning, navigation and timing (PNT) services. PNT services are addressed in the Space Sector because of the association of Global Navigation Satellite Systems (GNSS) with space. PNT services should correctly be associated with all sectors - Banking and Finance, Communications, Data and the Cloud, Defence industry, Education, Research and Innovation, Energy, Food and Grocery, Health, Space, Transport and Water.
2. Do you think the current definition of Critical Infrastructure is still fit for purpose?	The current definition is fit for purpose and we can easily link intent with all elements with Air Traffic Management – critical service and how aviation contributes to national economy.
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?	Recognition of the impact of utilities' interdependencies is required for agencies to understand the flow on effect to their business continuity. A rating's criteria should be developed for prioritising critical entities or classes.
4. What are the common threats you routinely prepare for and those you have faced/experienced as a business?	All 6 common security threats (trusted insider, organised crime, foreign intelligence services, issues motivated, fixated individuals and terrorism). –Airservices adopts an enterprise risk management framework to manage the risk to delivery of our functions and has developed the key risk scenarios that we routinely review through deep dives and control testing. Airservices continuously evaluates the cyber threat landscape for activity that could impact the operation of our core services. The dynamic nature of cyber threats necessitates a risk-based approach to decision making to ensure controls remain effective and relevant. Examples of prevalent cyber threats that Airservices actively prepares for and observes includes ransomware and malware attacks, phishing and web application exploitation. Similar to other organisations in Australia, Airservices continues to observe ongoing cyber attacks against our digital ecosystem.
5. How should criticality be assessed to ensure the most important entities are covered by the framework?	Criticality should be assessed by overall impact to society, economy and National security from the loss of services from entities. Consideration of service criticality is paramount to managing key risks. A criteria should be developed for determining what is critical.
6. Which entities would you expect to be owners and operators of systems of national significance?	We would expect any entity that owns critical infrastructure or systems (or operates these) should be directed by Australian Government policy.

7. How do you think the revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?	Reinvigorating the network of Practitioners of critical infrastructure will support the reforms by assisting entities to work and leverage off each other's interdependencies. CI Resilience Strategy will drive a common approach and engagement across identified sectors to achieve required outcomes.
8. What might this new TISN Model look like, and what entities should be included?	All entities considered under the new reforms should be considered in the TISN, maintaining each sector accordingly.
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?	Government can support CI entities by facilitating cross sector exercises/workshops, using more probable events in a short and sharp manner and which has overlay of cross dependencies from other sectors. More regular simulations and events rather than big scenarios based on worst case would provide more insights into actions required to improve business continuity arrangements
10. Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?	Principles are quite broad, accepting that there is a lot of supporting governance (e.g. PSPF, ISM, Supply chain risk).
11. Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?	The required security obligations appear to provide reasonable flexibility to apply a risk managed approach within the requirements but if there is a compliance requirement further defined then we'd need to understand cost benefit.
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?	Other Air Navigation Service Providers (ANSPs) are very aware of the cyber security principles as per the ICAO Annexure 17. As the principles are quite broad this allows industry to apply their own risk appetite and models, therefore also level of financial investment.
13. What cost would organisations take on to meet these new obligations?	The cost is difficult to identify at this stage however, organisations should focus on optimising their current practices and processes and developing organisational capability to enable them to respond to changing environments, in a fiscally sustainable manner, commensurate with sector risk profile.
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?	ICAO Annexure 17, PSPF and ISM – use the example of ASIC Program – regulators directing to meet security principles as compliance rather than risk base. Regulator needs to have a strategic understanding of all sector participants' dependencies and how we can demonstrate our risk management in adopting the principles and required outcomes.
15. Would the proposed regulatory model avoid duplication with existing oversight requirements?	Only if some of the current requirements are reduced (i.e. regulatory).
16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would	The regulator needs to understand our services and affect to national security etc. Also needs to understand modern cyber security resilience and how we manage risk. (Not a one size fits all). Engagement strategy needs to include this. Consistent

like to see included in this guidance, or broader communication and engagement strategies of the regulator?	messaging and all parts of the regulator providing consistent advice would be advantageous.
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?	Home Affairs through CI Centre and AMS could continue as regulatory body. A closer link between ACSC and other aspects of protecting CI. Regulator needs to understand the links between each agency within the sector (integrated).
18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?	Secondment opportunities for regulators so they can understand our business –service delivery limitations and drivers could be one initiative to help inform regulatory recommendations and compliance activities. Having an assigned individual that works with entities over a period of time – rather than a single guidance centre is a better mechanism for engagement between regulator and entities.
19. How can Government better support critical infrastructure entities in managing their security risks?	Government could better support CI entities in managing their security risks when heightened threat or risks are identified. There used to be funding available to CI entities that were struggling through significant change or crisis events to meet requirements – of course, a criticality approach would make this work smoother if reintroduced.
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?	We are very familiar with the AusCheck scheme as most operational staff require an Aviation Security Identification Card to access designated secure areas. Would be a great initiative for Home Affairs to consider sharing of information between Vetting agencies to provide security clearances that are recognised across all sectors (Police Checks, ASICs, National Security Clearances, Working with vulnerable people etc.) This would standardise requirements for critical infrastructure entities and reduce amount of personal information kept on individuals, (reduction of risk from personal/privacy breach) but also support staff moving between entities.
21. Do you have any other comments you would like to make regarding the PSO?	We fully support the concept PSOs with the understanding that clear criteria for obligations need to be agreed with industry. Development of PSOs should support the use of equivalent control sets, demonstrating a genuine approach to understanding how different organisations need to approach security challenges.
22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?	It is crucial that any positive cyber security obligations or frameworks are developed based on pragmatic and achievable cyber resilience outcomes for all critical infrastructure providers. A thorough evaluation of any proposed cyber controls should be undertaken against each organisation to assess feasibility and applicability as a “one-size-fits-all” approach is unlikely to result in an effective outcome.
23. What information would you like to see shared with critical infrastructure by Government? What benefits	Information that should be shared with industry includes actionable intelligence that provides organisations with the ability to take immediate action to protect systems and services from threats known only to intelligence agencies. The rapid dissemination of this intel is critical in securing Australian systems against cyber-attacks

would you expect from greater sharing?	quickly and effectively. Any sharing platform must support anonymization for participating organisations to maintain the integrity of the outcome.
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?	Airservices could contribute relevant telemetry such as non-attributable/redacted web, DNS and IP address values and other data via our Security Operations Centre. There would be cost implications such as web service configurations, redaction services and bandwidth costs to factor in to any proposed solution.
25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?	Traditional methods such as vulnerability scanning and software version analysis can provide one picture of an organisation's perimeter security, however strategic use of modern methods (such as cyber adversary simulations) are more effective in assessing an organisations cyber resilience. Modern-style engagements are better aligned to the tactics, techniques and procedures used by real adversaries as observed in the wild, and help properly evaluate organisational capability across prevent, detect and response categories.
26. What are the barriers to owners and operators acting on information alerts from Government?	Airservices does not experience any barriers in acting on cyber-related information provided by Government. Some information will not be actionable based on the type of systems Airservices operates.
27. What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?	Any playbook needs to be developed jointly between Government and each organisation. Incident response flows will differ across organisations, and Government will need to approach their development with flexibility towards process, risk assessment and function.
28. What safeguards or assurances would you expect to see for information provided to Government?	Any sharing of network or system related information is likely to be highly operationally sensitive, and also has the potential to be dynamic given the speed at which the industry is evolving. Accordingly, appropriately robust agreements would need to be put in place with government before such information is shared, covering such issues as: • What information is to be shared • How information is to be transferred • How it is to be stored • How it is to be accessed • Who may access it • Responsibility, obligations and liability of government in respect of any information share with them. Consideration needs to be given to whether any requested information is subject to existing third party confidentiality obligations which could prevent its disclosure.
29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?	Airservices position is that under no circumstances should Government or any other entity take any direct action that could cause disruption to safety-critical systems managed by Airservices without appropriate engagement and approval from duly appointed representatives within our organisation. Unintended consequences could result in significant safety issues for the Australian public.
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?	The National Security Committee or equivalent body would be an appropriate body to determine whether an activity should result in a state of emergency being declared. Who is first to provide advice is not relevant, rather it is crucial that an appropriately diverse selection of advisor groups are consulted before such decisions are made.

31. Who should oversee the Government's use of these powers?	The Parliamentary Joint Committee on Intelligence and Security or equivalent body.
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 the Government chooses to engage in offensive security operations against any nation, including Australia, legal and strategic advice should be sought prior to any offensive response.
33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?	It is difficult to provide a meaningful response without a clear understanding of what 'emergency actions' might entail, and the potential for harm (however inadvertent) such action may cause. Any immunity from civil action, for example, should be limited to specific, identified circumstances and should not extend to actions caused by the negligence or otherwise unauthorised conduct of the person seeking to claim the benefit of the immunity.
34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?	Exercise of any emergency action should be performed under the oversight of an appropriate, independent regulatory body. Depending on the circumstances or the proposed action, judicial oversight and review may also be appropriate, to ensure fundamental rule of law principles are followed.
35. What are the risks to industry? What are the costs and how can we overcome the? Are there sovereign risks to investment that we should be aware of?	Risks to industry (aviation) include: • Disruption of safety-critical services if direct cyber action is taken by Government without consultation • Diversion of funding from practical cyber control development and implementation to meet PSO requirements that may provide less protection than current controls • Financial impact to organisations with existing Long Term Pricing Agreements (LTPA) • Increased cost of providing telemetry to Government for unknown or non-existent benefit. Centralised funding models should be considered to ensure support is provided to CI organisations based on risk/required controls. Airspace management technology and support relies on both local and international technology partners with specialist capability, introducing the potential for sovereign risks. Effort should be made to understand the safety priorities of aviation organisations and potential impacts to national aviation safety should cyber be prioritised above the safety of air travel.
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?	Without a clearer picture on funding models, PSO structure and any mandated cyber requirements for CI organisations, these questions are not able to be answered.