Association Number A03958 | ABN 64 217 302 489

AUSTRALASIAN RAILWAY ASSOCIATION SUBMISSION

To the

Department of Home Affairs

On

Protecting Critical Infrastructure and Systems of National Significance – Consultation Paper

THE INDUSTRY

The Australasian Railway Association (ARA) is a not-for-profit member-based association that represents rail throughout Australia and New Zealand. Our members include rail operators, track owners and managers, manufacturers, construction companies and other firms contributing to the rail sector. We contribute to the development of industry and government policies in an effort to ensure Australia's passenger and freight transport systems are well represented and will continue to provide improved services for Australia's growing population.

The ARA and its members thank the Department of Home Affairs (the Department) for the opportunity to provide a submission on its Consultation Paper: *Protecting Critical Infrastructure and Systems of National Significance.*

This submission has been developed is consultation with ARA member organisations.

Any questions regarding this submission should be directed to Simon Bourke, General Manager – Policy, Research & Advocacy via [redacted] or [redacted].

GENERAL COMMENTS

The ARA recognises the need for the Australian Government to continually review and adapt its approach to protecting the essential services all Australians rely on for our ongoing prosperity, safety and security.

The ARA's members across the rail industry form a critical part of Australia's national transport infrastructure network. In a recent research report by Deloitte Access Economics (scheduled for release later this year) it found that in 2019 the rail industry contributed around $30 billion to the Australian economy and employed more than 165,000 workers. Over that same period the rail industry facilitated almost 1 billion passenger journeys across light and heavy rail, as well as moving over 425 billion tonnes of freight.

Australia's rail network remains critical to the movement of people, goods, and commodities across the country and within our metropolitan areas, with this task only expected to grow into the future. It is therefore essential that the rail industry be involved in discussions on the resilience of Australia's critical infrastructure.

The rail industry is currently subject to regulatory requirements at a federal and jurisdictional level for a range of issues, including cyber security. It is essential that any new federal regulatory requirements for rail entities regarding the protection of critical infrastructure recognise the existing processes in place in jurisdictions and minimise duplication and the regulatory burden imposed on industry.

It is also essential that for any information or data that industry may be required to provide government moving forward be subject to transparency regarding the purpose and use of the information. All sensitive information should of course be subject to strict privacy and confidentiality arrangements, which are made to clear to industry at the outset.

The ARA and its members are committed to working with the Government in the development of any new regulatory framework that seeks to enhance the security resilience of our transport network in an efficient, effective and affordable manner.

REPSONSES TO SPECIFIC QUESTIONS

The following outlines some comments and suggested changes to specific parts of the draft

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 ARA believes that the sectors outlined in the Consultation Paper broadly capture the functions that are vital to Australia's economy, security, and sovereignty. Manufacturing may need to be considered in a local context to the extent that it may be critical to the ongoing viability of certain sectors with critical and time sensitive supply chain requirements.

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

The ARA acknowledges that the current Critical Infrastructure definition remains fit for purpose in that it captures the facilities, networks and systems that are critical to Australia's economic and social wellbeing.

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?

The ARA believes that assessing interdependencies with other functions, as well as the consequences of compromise, will provide a useful mechanism for identifying and prioritising critical entities and classes. It should be noted that the mapping exercise itself may also reveal additional factors or parameters that would be worthwhile considering. This should be recognised with sufficient flexibility built into the mapping process.

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

The ARA's members undertake a variety of incident and threat response preparation activities. These include (but are not limited to) train/rail network disruptions, telecommunication network outages, and multi-agency emergency/threat exercises.

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

The ARA believes that criticality could be assessed by conducting a likelihood and severity of consequence assessment. In determining severity of consequence, factors such as the threat to life, threat to environment, and threat to economic activity should all be considered.

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

Due to the significantly varied ownership and operator structures of nationally significant critical infrastructure systems, it is reasonable to expect that these systems would have a combination of federal, state and local government entities and private companies in control. Noting that all owners and operators of such systems are subject to significant regulatory oversight.

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

The ARA believes a revised TISN and Critical Infrastructure Resilience Strategy would assist with creating a more robust, coordinated, and strategic approach to the sharing of critical information and developing a more comprehensive understanding of the threat environment.

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

The new TISN model may benefit from a layered approach as outlined in *Figure 1: Classes of Entities* to include representatives from each of those sectors and direct links back to relevant industry bodies. This type of structure would ensure the type and level of information provided was fit for purpose for each class of entity.

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?

The ARA believes there would be benefit in government providing additional support to assist industry in obtaining a more detailed understanding of the interfaces and interdependencies between critical infrastructure systems. This may be in the form of educational training/workshops that explore risks, obligations, and requirements associated with those cross-sector interface points.

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

The ARA agrees that the principles-based outcomes outlined in the consultation paper are sufficiently broad to capture the security risks and protect entities from all hazards.

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

The ARA believes that both the physical security and cyber security obligations outlines in the consultation paper provide an appropriate balance in providing clear expectations with sufficient flexibility to implement.

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 information received by ARA from its members indicated that a number of large businesses within the rail industry are already broadly operating in-line with the security principles in the consultation paper. However, the time and financial burden on businesses to meet these principles will likely depend on the level and nature of monitoring, auditing, and reporting required to demonstrate compliance. The ARA recommends that existing systems and process be utilised to demonstrate compliance wherever possible in order to minimise duplicative requirements.

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

The costs that organisations in the rail sector are likely to incur would be related to personnel, IT systems upgrades/maintenance (hardware and software), and additional staff training.

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 comment.

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

Considering the diversity of sectors involved in the provision of critical infrastructure and the regulatory requirements involved, the proposed regulatory model may avoid some duplication with existing oversight requirements. However, it will most likely be necessary to undertake a detailed mapping exercise of existing regulatory requirements across the impacted sectors to avoid duplication.

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?

It will be important for any guidance issued to industry to be detailed and practical, with a focus on best practice and a degree of flexibility to account for different business operations. Wherever possible it would be beneficial to have coordination across jurisdictions and different regulators to ensure a more seamless and integrated adoption of measures.

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?

For the rail sector there is currently no obvious existing entity that could undertake this regulatory function without significant change. The rail sector currently has the Office of the National Rail Safety Regulator (ONRSR), however their remit is focussed solely on the safety of the network, rather than matters related to security protocols. The ARA believes it is critical that a key priority must be to avoid duplication of regulatory functions between federal and state entities, with a clear, practical and consistent process for industry to adhere to.

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

No comment.

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

The ARA believes regular briefings, communications and guidance is critical to assist critical infrastructure manage their security risks. There would be value in briefing industry on changes in the threat environment relevant to their sector (including learnings from incidents in other sectors) and ensure there is consistency between state and federal government regulatory requirements.

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?

The broadening of the AusCheck scheme (or similar) should only be considered through a risk-based approach on sector by sector basis, with clear linkages to a change in the threat environment for that sector. While the Auscheck scheme is useful for undertaking background checks for new employees, it is significantly limited by the fact it has no on-going monitoring capability for changes in criminal records to notify the employer. This is currently an issue for ASICs in aviation and MSIC in maritime. The costs for industry associated with these schemes are also significant.

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

No comment.

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

There may be value in testing the effectiveness of the proposed 'playbooks' to ensure that that communication and action protocols are practical and effective. This could be incorporated into the proposes cyber security activities.

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

See answer to question 19.

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?

Members of the ARA are likely to have varying capabilities in terms of contributing to the threat picture, however those that can would likely be willing to do so on a voluntary basis.

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

No comment.

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

The barriers may include the resourcing and capability within the organisation to understand and act upon the information provided. This is likely to vary depending on the level of security requirements currently imposed on the organisation.

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

The ARA believes that the playbooks could benefit from considering specific response tactics, mitigations, notification procedures and fallback scenario plans. Th systems architectures in place between government and industry may prove challenging to co-development in some scenarios.

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

Adherence to best practice and regulatory requirements for the sharing of sensitive data and information, including respecting privacy provisions and ensuring information is only used for its intended purpose.

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

The ARA believes that these situations need to be subject to detailed discussion with the potentially impacted entities directly, given the potentially significant ramifications for the organisations involved. At a high level, any such actions should only be considered in situations the equivalent of a 'State of Emergency/Disaster".

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 declaration of an emergency would be most appropriate from the Federal and State Governments, however this should be done in close collaboration with the industry participants involved/impacted.

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

No comment.

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?

No comment.

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

No comment.

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

No comment.

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?

See response to question 29.

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?

See response to question 29.