Submission

To

Critical Infrastructure Centre’s
Strengthening the National Security of Australia’s Critical Infrastructure
Discussion Paper

March 2017

Submitter: Paul Daly
Chief Executive Officer

Organisation: Rail Industry Safety and Standards Board

Address: PO Box 4271 Kingston ACT 2604

Phone: [redacted]

Mobile: [redacted]

Email: [redacted]
BACKGROUND

1. The Rail Industry Safety and Standards Board (RISSB) is a not for profit, member owned organisation. Under the co regulatory system of the Australasian railway networks, RISSB develops and manages the Australian Standards, Codes of Practice, Guidelines and the Australian Rail Risk Model and the National Rules for the rail industry. RISSB is committed to developing quality products in line with industry needs, the public interest and harmonisation.

2. Established in 2004, RISSB is a Standards Development Organisation (SDO) and is accredited by Standards Australia to develop standards for the rail industry. As such RISSB is the only organisation in Australia that can produce Australian Standards for the rail industry.

3. RISSB is a member based organisation. with its membership representing more than 95% of the rail industry in both Australia and New Zealand, and includes rail operators, infrastructure managers and operators, freight and metro companies and suppliers.

4. RISSB is appreciative of the opportunity to submit its views on the Strengthening the National Security of Australia’s Critical Infrastructure Discussion Paper. In our submission, we have shown how rail meets the definition of critical infrastructure, and have proposed several initiatives that will provide for a strengthening of security around them.

RISSB SUBMISSION

The Rail Industry in Australia

5. The Australian rail networks are the world’s sixth largest, with more than 33,000 route kilometres. The majority of this is owned by governments (both State and Federal) with a quarter of the network managed and maintained by the Australian Rail Track Corporation (ARTC).

6. While the Australian networks are predominately used for heavy haul (this includes freight along with coal and iron ore), Australia’s metro systems undertook more than 644 million passenger trips in the 2014/15 financial year. Of these over 292 million were undertaken in Sydney alone (Australia’s busiest metro).
7. During the same financial year, Australia’s rail freight companies carried some 1.2 billion tonnes of freight, 62% of which was iron ore in Western Australia, and 29% was coal in New South Wales and Queensland. Other freight included grain, livestock, vehicles and general freight.

8. The figures above show that 91% of all freight carried were export goods carried as part of the supply chain to Ports on the east and west coasts of Australia.

9. During the 2014/15 financial year, Australia’s export earnings from resource and energy commodities totaled $174 billion, with Australia being the world’s largest exporter of iron ore, accounting for 53 per cent of world trade, and were the second largest exporter of coal. All of which was carried from “pit to port” by rail.

10. While Australia’s economy already relies heavily on the rail industry to transport its goods, rail freight is expected to increase by 60% between 2010 and 2030. To manage these increases in demand, owners and operators are focused on secure and efficient asset management, development of comprehensive distribution lines and innovations to combat the vast distances and harsh landscapes the rail industry operates in. Realisation of this need is demonstrated with the development of the Pilbara lines, the development of the Melbourne to Brisbane Inland Rail, the extension of the Hunter Valley network, and the forward planning for the Carmichael Coal rail line.

11. Passenger rail plays an integral role in Australia’s economy, with Australian Census data showing that more than one third of workers across Australia’s capital cities rely on the rail network to get them to and from work. This number increases to 45% in Melbourne where workers also have the option of commuting on the world’s largest light rail (tram) network. As Australia capital cities develop and expand their light rail systems, this number of commuters will increase exponentially.

12. Over the past decade, the Australian rail network has become more reliant on computer based systems such the European Train Control System (ECTS) to manage the movement of trains across all aspects of the network, including those sections of the network where freight and passenger services interact. In the coming decades, driverless trains and light rail systems will place even more reliance on the use of automated control products, with the potential to leaving an entire network vulnerable to espionage, sabotage and coercion.
13. Throughout the Discussion Paper, and across supporting documents such as the Critical Infrastructure Resilience Strategy (Policy Statement and Plan) and the National Guidelines for Protecting Critical Infrastructure from Terrorism, the Australian, State and Territory governments share the definition of critical infrastructure which is;

“those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia’s ability to conduct national defence and ensure national security”

14. RISSB believes the Australian rail network, be it that which carries freight or that which carries passengers to and from work, falls into this definition.

15. The Australian rail networks are an important element of critical infrastructure that integrates elements such as port, power and people through the supply chain. In the Discussion Paper the Critical Infrastructure Centre notes that Australian Ports are critical infrastructure as “Australia relies heavily on its commercial ports to trade goods with the world, with one third of GDP facilitated through seaborne trade”. As shown above more than 90% of rail’s heavy haul terminates at a port in Australia.

16. With one third of all capital city workers relying on rail transport to commute to and from work, the destruction or unavailability (even for a short period of time) of a capital city metro train service would have huge detrimental effect on the companies based in capital cities.

17. In September 2013, the Transport and Infrastructure Senior Officials Committee (TISOC) tabled the National Surface Transport Security Strategy. In the strategy TISOC speak of the threat context to rail, and state;

Surface transport systems are attractive terrorist targets, because – depending on the nature of the transport operation – they may fulfil a number of the following criteria;

- These systems present a high potential of mass casualties
- Transport systems are by their nature open to the public, very accessible and vulnerable to attack.
- An attack on a transport system could have a significant economic impact.
- Spectacular imagery is likely to be generated.
- There is significant opportunity for attack and likelihood of success.
- An attack against a transport system would make a symbolic statement that would resonate with terrorist objectives and the targeted communities.
- An attack would generate significant public fear and anxiety.
18. This demonstrates the effects of an attack on Australia’s rail networks, be it a terrorist attack or a cyber-attack on the network’s train control systems would generate the detrimental effects to the nation’s economy and wellbeing characterised in the definition of critical infrastructure.

19. Unlike other critical infrastructure in Australia, the rail network is the only physical facility that carries passengers, inclusive of commuters, tourists and the general public, and therefore is the only infrastructure in Australia that has the potential for mass casualties and deaths caused from an attack against it.

RISSB responses to questions raised in the Discussion Paper

20. As mentioned above, RISSB will not respond to all the questions raised by the Discussion Paper, but only those where it believes it can add value to the discussion.

Are the proposed functions of the centre adequate to better manage the national security risks to our critical infrastructure?

21. RISSB believes that the key functions identified in the Discussion Paper are a solid foundation on which to build a more inclusive network of protective security and risk mitigation measures.

What role could you play in assisting the Centre to undertake these key functions

22. RISSB believes it can play a vital and extremely beneficial role in assisting the Critical Infrastructure Centre achieve its objectives.

23. RISSB works closely with its international counterparts (such as the Rail Safety and Standards Board (RSSB) in the UK) and is aware of cyber breaches that have been attempted overseas, and what other standards and safety bodies are developing to mitigate these threats to their national infrastructure.

24. As mentioned above, heavy and light Rail in Australia are managed through Control Systems both in signaling to regulate rail traffic by speed/distance and to operate infrastructure components such as points to set the route. These are predominately managed through digital software and information technology interfaces.
25. With legacy systems in place and new technology being implemented on the Australian rail network such as European Train Control System (ETCS) and High Capacity Signaling (HCS), it is now more important than ever to ensure that all operating systems are protected from any attempted cyber security breach.

26. RISSB believes that the correct approach should be to mitigate the risk across the entire rail transport networks, not just signaling systems, and identify and address all elements that are used in the operation of a railway, including rolling stock, information systems, and the infrastructure itself.

27. This would also include the housing of systems, the protection of assets from a set location and the security of these locations.

28. Through collaboration with its international associates, RISSB has already identified Cyber security breaches that could result in the following:
   - Mass deaths and casualties
   - Threats to safety
   - Disruption to network operations
   - Economic loss to operators, suppliers and the wider Australian community
   - Reputational damage to rail organisations and government
   - Loss of commercial and sensitive information
   - Criminal damage

29. Further Discussions with industry has provided a list, of the areas that should be considered including:
   - Details the underlying performance requirements of Train Control Systems
   - Manage the security of Train Control Systems
   - Manage vital safety systems
   - Manage non-vital signaling systems
   - Manage system availability
   - Third party networks and self-managed networks
   - Interfaces to corporate networks (Management Information)
   - Remote access points for support
   - Train radio systems
   - Rolling stock systems
   - CCTV security systems
   - Passenger information systems
   - Building management systems
   - Electrical system points and locations
   - Training and awareness
30. Victoria’s Audit Generals Report 2016 *Security of Critical Infrastructure Control Systems for Trains* notes that significant weakness in the security of control systems of train operators within Victoria. In addition, the report detailed no Australian Rail Standards, Guidance documents or frameworks in place to support the rail industry in Australia.

31. RISSB has been requested by industry to develop a suite of documents in the form of Australian Standards and Guidelines to assist industry in combatting cyber-attacks on the Australian rail network. These needs are based on the concerns of the management of this risk, and the potential for catastrophic outcomes if nothing is done in this area.

32. RISSB would look to engage the same collaborative approach to achieving this outcome and would seek to support the industry in managing the risk of cyber attacks and encourage operators, infrastructure managers, suppliers and contractors to apply the appropriate risk mitigation controls (defence) through a national program of work.

33. In the initial high level research, RISSB will provide a national program of work which includes the following elements as part of a work program to assist industry:

- Cyber Security Framework
- Standards and guidance documents
- Support industry developed operational guidance
- Tools (risk profiling, assurance/assessment, data collation, etc.) and supporting materials
- Training programs and materials including delivery to operators
- Assurance programs

34. RISSB aims to support the Australian Governments Cyber Security Strategy 2016 through this work program, and believes that the work program outlined above complements the plans outlined in the *Critical Infrastructure Resilience Strategy: Plan*, particularly the words on page two of the Plan which state;

> The Australian Government advocates the use of relevant international, Australian and New Zealand Standards for Risk Management by owners and operators of critical infrastructure, for example AS/NZS ISO 31000:2009

*How should the Centre work with owners and operators when performing its functions, including understanding existing mitigation mechanisms?*

35. RISSB believes it can further assist the Centre in this area by providing advice and recommendation on existing and future mitigation mechanisms on an industry wide basis.
36. There are differing regulatory formats ranging from self-regulation to full regulation. Under a co regulatory system, such as that currently applicable to the rail industry, critical infrastructure owners, managers and end users are empowered to utilize their own safety and risk mitigation processes to demonstrate compliance to a safety regulator.

37. This is achieved through a collaborative approach to safety and security. RISSB believes that this system works well, and would support the Centre in adopting this style of collaboration in the execution of its functions.

What other types of information would improve our understanding of foreign involvement in outsourcing, offshoring and supply chain arrangements?

38. RISSB is mindful, and wishes to bring to the Centre’s attention, that the Discussion Paper made no reference to the construction or maintenance of critical infrastructure, that is to say, who the manufacturers of equipment installed in the infrastructure are, and who are the secondary users of the infrastructure.

39. In the example of the rail networks, much of the signaling and train control systems are designed, implemented and (on occasion) commissioned by foreign companies with little or no presence in Australia.

40. RISSB believes that these aspects of a critical infrastructure asset, where relevant, may fall under the purview of the Asset Register.

Does the 30 day period provide sufficient time for owners to register their interest in a critical infrastructure asset? If not, what alternatives do you propose and why?

41. RISSB does not believe that 30 days would be sufficient for owners to register their interest in critical infrastructure assets given the complex business transactions and time it takes for the transfer of ownership of these types of assets.

42. RISSB believes that a period of 60 to 90 days would allow for more accurate reporting to the register.
Is a six month transition period appropriate? If not, what alternatives do you propose and why.

43. RISSB believes, until more detail is provided by the Centre on exactly what it requires from owners and manager for the register, a twelve month transition period would be more appropriate.

What are the main advantages and disadvantages of a register administered by the Australian Government?

44. RISSB is unsure it sees a clear benefit to the development of a register, and is unclear as to exactly what critical infrastructure would be included on the register, and how compliance would be policed.

45. Duplication of reporting would also be seen as a disadvantage to many companies, with the obvious cost implications that are driven by compliance.

46. That said RISSB is keen to know more of the intentions and mechanics of the register before it makes a decision on it.

What are your views on the introduction of a “last resort power” to address significant risks where all other risk management avenues have been exhausted?

47. RISSB would seek further information on the implementation of “last resort power”, having concerns with regard to the generalization of risks and inaccurate categorizing of risks which may lead to reputational damage and reduce confidence in foreign investment.

CONCLUSION

48. RISSB fully supports the work being undertaken by the Australian Government to protect this nation’s critical infrastructure.

49. RISSB believes that the Australian Rail Network clearly falls within the Australian Government’s critical infrastructure definition, A targeted attack on rail infrastructure would have a detrimental effect on the nation’s economy if disrupted, degraded or destroyed, but can also see large scale loss of life and mass casualties as potential ramifications to an attack on the networks.
50. RISSB stands ready and willing to assist the Critical Infrastructure Centre regarding mitigating the risks this submission has highlighted already exist in the rail industry.

**RISSB CONTACTS**

51. The Rail Industry Safety and Standards Board would like to thank the Critical Infrastructure Centre for the opportunity to tender its submission to the Discussion Paper.