V/Line Business Overview:

V/Line, as a brand, has provided public transport services to regional Victoria for over 30 years. Each week, V/Line schedules more than 1,997 train services between Melbourne and:

- Geelong and Warrnambool
- Ballarat, Maryborough and Ararat
- Bendigo, Swan Hill and Echuca
- Seymour, Shepparton and Albury
- Traralgon, Sale and Bairnsdale.

More than 1,462 V/Line-branded coach services connect with the rail network and serve regional Victorian communities. Some of our coach services, under normal circumstances, also link Victoria with South Australia, New South Wales and the Australian Capital Territory.

As well as being a public transport operator, V/Line also leases, provides access to and maintains over 3,520 kilometres of rail track used by passengers and freight rail operators.

Current Standards and Context:

Purposes of ONRSR and RISSB within the Rail Environment

The principle regulator for the Australian rail industry is known as ONRSR (Office of the National Rail Safety Regulator). As outlined in the 'ONRSR Statement of Intent 2020-2023' ONRSR provides the following to the industry:

"ONRSR administers the Rail Safety National Law and performs the functions and responsibilities conferred upon it by that law.

The overarching intent of ONRSR is to improve rail safety for the Australian community and the delivery of seamless national rail safety regulation of rail operations."

Conversely, standard's applicable to the Australian rail industry are developed by RISSB (Rail industry Safety and Standards Board). As per the RISSB website, their role within the industry is:

"RISSB is the only accredited Standards development organisation for the rail industry in Australia"

Within the RISSB product catalogue are the following standards:

- AS 7770:2018 – Rail Cyber Security
- AS 7770: 2018 - Rail Cyber Security Guideline
- Code of Practice - Rail Cyber Security for Rolling Stock & Train Control Systems, (2020)

Although the RISSB is the accredited body to develop standards for the rail sector it does not have the ability to enforce such standards and, unfortunately, are not recognised by parties involved in the delivery of capital projects.

The review and development of Federal Critical Infrastructure Legalisation should include the standards governing body for the industry not just the regulator.

Office of the Victorian Information Commissioner (OVIC)

The Office of the Victorian Information Commissioner, (OVIC), is an independent regulator with combined oversight of information access, information privacy, and data protection. As the primary

regulator and source of independent advice to the community and Victorian government about how the public sector collects, uses and shares information, any review and development of Federal Critical Infrastructure legislation should also consider OVIC; in particular it's impacts on the *Privacy and Data Protection Act 2014 (PDP Act)*, namely the Victorian Protective Data Security Framework and Standards (VPDSF and VPDSS) that V/Line must comply with as part of the Victorian public sector.

Victorian Protective Data Security Standards – VPDSS:

Standard 1 – Information Security Management Framework
Standard 2 – Information Security Value
Standard 3 – Information Security Risk Management
Standard 4 – Information Access
Standard 5 – Information Security Obligations
Standard 6 – Information Security Incident Management
Standard 7 – Information Security Aspects of Business Continuity and Disaster Recovery
Standard 8 – Third Party Arrangements
Standard 9 – Information Security Reporting to OVIC
Standard 10 – Personnel Security
Standard 11 – Information Communications Technology (ICT) Security
Standard 12 – Physical Security

As a Victorian Public agency, under the portfolio of the Department of Transport (DoT)), V/Line Corporation regularly attest to the Office of the Victorian Information Commissioner with our Protective Data Security Plan (PDSP). (Last attestation dated Aug 2020)

The PDSP aims to

- Assess our organisation's information security capability;
- Summarise our progress towards our implementation of the Victorian Protective Data Security Standards (VPDSS); and
- Provide assurance to the Office of the Victorian Information Commissioner (OVIC) that our organisation is making progress to improving information security.

V/Line currently alert OVIC when a cyber security incident is detected. And participate in the Information Security Advisory Group (ISAG), which is sponsored by the Department of Premier and Cabinet (DPC): This group aims to provide advice, guidance and resources to all Victorian Government entities with respect to cyber.

Observations on Proposed Legislation Changes and Regulated Practices:

The State Legislative Framework

The surface transport sector is a rich and diverse one, embracing freight and passenger movements across multiple modes. Component parts of the portfolio have differing regulatory obligations, subject to their respective industry, national and state governing mechanisms. Having regard to the state of Victoria, a number of transport entities, embracing road, heavy and light rail, as well as communication service providers, have been designated as 'Vital' critical infrastructure. The state uses a tailored assessment instrument, the Victorian Criticality Assessment Tool, (Vic-CAT), to determine infrastructure categories, from Vital to Local.

Within the current proposal, there is a lack of clarity around definition of criticality and the identified thresholds: Specifically, what is the meaning of 'capable', in a public transport context? Also, the definition of 'freight transport' for inclusion is loose and lacks rigour; in this environment an assessment around service provision would probably be more appropriate, rather than a revenue based threshold.

Identified 'Vital' entities in the transport sector embrace both state government and private operators, who are subject to regulation, under the provisions of Part 7(a) of the Victoria Emergency Management Act 2013. Obligations include the conduct of an annual exercise, an independent audit of emergency management plans systems and processes and the production of an assurance and attestation statement to the portfolio department, the Department of Transport; the latter details activities and initiatives undertaken, and planned, pursuant to the continuous improvement cycle. The legislation has an 'All Hazards' approach, which includes security threats and risk management.

Any Federal legislation must take account of those processes already in place, across the different jurisdictions, in order to prevent duplication of effort and an unnecessary regulatory burden on the operator community. Levels of maturity will differ between the states and territories, making universal implementation of measures, and the avoidance of repetition and needless bureaucracy, difficult to achieve. An individual state by state approach potentially belies the overall intent of Federal regulation, though such an approach is required, if duplication and unwanted regulatory compliance are to be avoided.

The Application of Standards

In many respects, making individual operators the focus of regulation can be argued to miss the point. In a great many circumstances, such entities are, to a large extent, caretakers of infrastructure delivered to them by state and Federal projects through public- private partnerships. These entities are not currently understood to be part of the legislative equation, though their involvement in the delivery of multi-billion-dollar investment by governments, is pivotal in determining the veracity of security architecture and infrastructure.

Feedback from several participants in conducted workshops have provided that the application of standards is vital in ensuring the security and protection of the nation's assets, infrastructure and data. It can be effectively argued that the most effective implementation of standards occurs in the project concept and construction phase.

Having regard to assets of national significance, and the current levels of investment in surface transport infrastructure, such ventures are delivered through government and industry partnerships, alliances and agencies. These entities, however, do not currently feature within the proposed legislative boundaries. The inference, and effect, being that such partnerships can continue to deliver sub-optimal infrastructure, without any application of standards, which operators then inherit and are subjected to regulation on their management. Such a position is as unfair as it is ineffectual, when considering the intended outcome of the proposed legislation.

Anticipated security legislation provides an opportunity for government to make a real difference, rather than simply provide for a bureaucratic overlay that delivers an illusion of efficacy. Basic security standards must be established for all new build, and upgrade, government projects. Their present omission provides a mixed bag of infrastructure security outcomes. Some projects bear a strong security hallmark, whilst others pay lip service, or have no discernible features at all. All too often, security is the first casualty in the face of project cost cutting measures, leaving end user

operators with substandard products, which deliver consequent outcomes. Having these entities then bear the burden of regulation and compliance is inequitable and unsustainable.

If the agents of infrastructure delivery are not to be formally embraced by new legislation, there at least need to be accompanying guidelines which they must be held accountable to. Such guidelines should articulate minimum standards, drawn from industry, and international, best practice. Guidelines might also recommend the appointment of security architects for major projects, the threshold for which will need to be determined. The UK Cross Rail project employs specific skills and expertise with oversight of the delivery of security components. The UK also produces guidance materials for significant rail projects, embracing physical security principals, based on Crime Prevention Through Environmental Design, (CPTED). The UK Government has recently re-issued the Security In the Design Of railway Stations, (SIDOS), Guide, to help inform construction projects. There is much for us to learn from these examples, to ensure our own infrastructure has security woven through its design and delivery, in terms of both cyber and physical attributes.

The RISSB adopted all the standards and best practices as well as industry Codes of Practices as defined by the Australian Government which are reflected within their security manuals, including SIDOS and the UK Centre for the Protection of National Infrastructure, (CPNI), guidelines.

Similarity, the European Union's (EU's) introduction of the Network Information and Security (NIS) directive in 2016 was the first piece of EU-wide legislation on cybersecurity, proving legal measures to boost the overall level of cybersecurity within Europe. This focused on setting a range of security requirements which apply to Operators of Essential Services (OES), including enterprises in the energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure sectors.

The Inter-Governmental Agreement on Surface Transport Security and the Trusted Information Sharing Network.

Guidance might best be delivered through a re-crafting of the Inter-Governmental Agreement, (IGA), on Surface Transport Security, which has not been properly reviewed since 2013. To be effective, any future strategy for the surface transport sector must adequately set out the role of state government; not only in respect of existing and potential responsibilities as regulators, but also as owners, operators and deliverers of critical infrastructure.

A reinvigorated IGA may go some way toward addressing these issues. In addition, connecting government and operator responsibilities could be achieved through a more robust Trusted Information Sharing Network, (TISN), process, which has become less relevant over recent years. Judicious use of both the IGA and TISN perhaps represents a solution to some of the Constitutional limits on the Commonwealth's ability to legislate in the transport sector. These mechanisms would require substantial work to make them more relevant per se, as well as means to garner and coordinate effort across a complex sector, embracing multiple actors, interests and responsibilities. Notwithstanding that both have been allowed to stagnate almost to the point of irrelevance, eroding trust in their overall effectiveness.

Regardless, the introduction of legislative imperatives can be argued to be capable of breathing new life into these processes. A partnership between all three perhaps represents the best, and only, real way of delivering on the outcomes outlined in the consultation paper, at least as far as the surface transport sector is concerned.