Ref: 201123_Consultation_CI_Amendment Bill
25 November 2020

CI Reforms
Department of Home Affairs
[redacted]

To whom it may concern;

Re: Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

Thank you for the opportunity to make a submission on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

As a surface / public transport operator and the proud operator of Yarra Trams, the world's largest light rail network, we understand and support the improvement and continuing resilience of critical infrastructure.

After attending the Townhall 3, this submission takes the form of general feedback and has been compiled with input from key internal stakeholders.

Not to Duplicate existing regulatory security programs.

Whilst the intention not to duplicate existing regulatory security programs is mentioned four times within the Explanatory document (s8, 21, 42, 263) this undertaking is not addressed within the Bill.

Industry must have a guarantee that duplication of process will not occur. This undertaking should be enshrined within the Act.

'Switch-On' of Part 2 rules

Within this Bill, one of any 11 Sectors that fall within the various definitions of Critical Infrastructure (section 8D) is subject to the arbitrary decision by the Minister of Home Affairs with respect to the 'Switch-On' of Part 2 rules and the imposition of the three separate requirements. If imposed, a business will be granted a six-month grace period in which to comply.

Although there is some reference to consultation with business, regulators, peak bodies and sector groups, there is no detail on the criteria or context in which this 'Switch-On' may or may not occur. Without having 'Switch-On' criteria documented, industry is unable to make a judgement as to the likelihood of being 'Switched-On' and therefore face the dilemma of having to decide on preparing or not preparing for Critical Infrastructure Part 2 requirements, without the adequate advanced information for making the decision.

Business and financial logic will direct many businesses to take a wait and see approach to developing plans for implementing Part 2 rules that may impact upon operations, whilst on the

other hand the six months offered by the Department to comply is very little time in which to identify, design and develop processes and procedures to support the Part 2 requirements.

Industry require clear criteria for the 'Switch-On' decision-making activity by the Minister, it should not be discretionary.

Monitoring compliance to the requirements.

During Townhall 3 the audience were given a verbal assurance that the Department were to take a 'Light Touch' approach to monitoring compliance and that 'Self-Declaration' was the preferred option.

Given that many existing workplace safety programs and regulations, require the person in charge of the business (i.e. CEO) to be the responsible person for the application of safety and security legislation, why would Home Affairs wish to move away from normal convention to an excessive requirement. Section 30AG 2(f) that; *if the entity has a board, council or other governing body—is signed by each member of the board, council or other governing body, as the case requires.*

If self-declaration is to be the principle manner of reporting compliance, this responsibility should rest with the CEO or equivalent – consistent with industry practice.

Background checks.

Section 30AH (4) *Rules made for the purposes of paragraph (1)(c) may require that a critical infrastructure risk management program include provisions that require background checks of individuals to be conducted under the AusCheck scheme."*

This level of clearance is excessive for most businesses, including those declared Critical Infrastructure. This is more akin to the needs of 'Systems of National Significance'.

As many organisations already utilise the Protective Security Policy Framework (PSPF) as guidance, the PSPF Personnel Security Clearance is appropriate and, in most cases, would not incur additional expenses.

30AH (4) would be better received if reworded to identify this AusCheck level of clearance for 'Systems of National Significance' and not across all businesses. The current wording is misleading.

Conflict of interest.

There are instances where State and Local Governments have engaged private enterprise, statutory authorities or government owned enterprises to operate services.

This applies across business, including electricity, water and transport, where private enterprise operate infrastructure and services on behalf of government. In the case of Yarra Trams there are existing contractual and reporting requirements with the Victoria Department of Transport, associated with the Franchise Agreement for the operations of Yarra Trams.

There must be safeguards within the Bill addressing any potential conflicts of interest where an entity or government authority having a financial interest are not placed in the position of potential conflict through the oversight of the Critical Infrastructure Bill.

Review or Appeal on Department Critical Infrastructure decisions impacting business.

There is no detail as to any measures within the Act for review or appeals of Department decisions. Business should have the right to review and Ministerial decision appeal enshrined within the Bill.

General observation

Security is a holistic management process and none of the facets of security risk management should ever be prioritized over other aspects.

There is considerable detail and specific requirements documented by Home Affairs in this Bill with respect to the Cyber Security issues within Critical Infrastructure. The other pillars of security (physical, personnel and information) receive far less attention, as do the 11 new categories of Critical Infrastructure (section 8D), which on the surface all appear to be afterthoughts.

Although there are clearly defined requirements for cyber security within this Bill, the Department would be well served to also commit the same level of attention into specifying physical and personal security minimum standards for the protection of material assets. Assets, that if interfered with, damaged or destroyed would have severe consequences on the critical infrastructure and potentially the national supply chain.

There is a clear need for a more balanced approach to Critical infrastructure, holistic security.

Care must be taken to ensure that regulation and legislation are not prohibitive to the successful operations of any enterprise.

We appreciate the opportunity to contribute to this process and look forward to joining the workshops further in the year.

Yours sincerely

[redacted]

Peter Boyce

Advisor, Security

[redacted]

[redacted]