Introduction

This response is a collective view from FASE to address the issues raised and make recommendations in response to the Critical Infrastructure Legislation Exposure Draft 2020.

Founded under the name SECMAN in 1999 and expanded and renamed in 2016, FASE has evolved into a professional affiliation of corporate security executives, occupying the most senior national and/or regional security role in their organisation; with responsibilities relating primarily to Security and Business Continuity Management, inclusive of Crisis and Emergency Management. Members other functional responsibilities may include internal investigations, fraud, cyber security and operational risk management. There are 50+ member companies, with national and/or international standing with an individual annual turnovers in excess of one billion dollars.

A list of companies can be supplied on request.

FASE aims to achieve three primary goals in its pursuit of security best practice; by sharing knowledge and insights in the following ways:

- Promoting a trusted environment for Australian corporate security executives to discuss contemporary and strategic security threats and risks;
- Ensure collaborative engagement with all levels of Government and industry stakeholders on strategic security issues; and
- Provide security leadership and trusted advice on matters of national strategic importance by harnessing the collective experience, knowledge and resources of its members.

26 November2020

FASE Executive

Chair Nicholas Martin (AGL) [redacted]
Deputy Chair Jason Brown (Thales) [redacted]
Secretariat Melanie Power (Virgin Australia) [redacted]

Protective Security Response

FASE welcomes the legislation and the move to a clear principles-based risk managed approach to critical infrastructure Resilience (CIR). It continues to seek to minimise regulatory impact and number and level of intrusive regulatory requirements and supports the flexible and consultative approach inferred throughout the explanatory document.

FASE members have had opportunity to examine the submission from AI Group, to which a number of companies are active members. As a collective the FASE membership supports the position taken by AI Group and would wish to offer some additional suggestions to improve management and reporting on the relevant security components of the changes. While our previous comments on the discussion paper are of continuing relevance to Legislative implementation and regulatory framework It is not intended to reproduce the proposals made in our previous submission.

Reference is made to specific paragraphs in the explanatory document on the Bill and as required to any item in the Bill itself.

Paragraph 6 of the document, dot points 1 and 2, address the positive Security obligations and the Enhanced Cyber Security Obligations. As illustrated in diagram 1, it is the combination of security controls that provide a comprehensive positive security outcome when effectively integrated with governance and guided by risk management. Cyber security does not sit in isolation of personal, physical and tangible information security processes. The relationship between cyber security reporting and mitigation is part of the security cycle and needs to be articulated as such. Refer our previous submission.

It is suggested that in directing CI industry participation a holistic security approach be adopted and all security obligations be under the same reporting and governance arrangements, particularly if CEO or Board level sign off is required by way of attestation. It is suggested that the Nominated Empowered Accountable Security/Resilience Executive at C suite level or equivalent should be the point of convergence of all security practice domains. The Chief Security Officer (CSO) or equivalent is an appropriate point of contact for policy and procedures and tactical and operational actions.

This approach will allow for better implementation of the partnership arrangements outlined in paragraph 8 where the private sector expertise in the company's security posture and competency is recognised through such an Accountable Officer.

In respect to paragraphs 17 to 20 the continuing linkage between an all hazards approach, which enhances resilience, and expansive risk management while correct in establish expectations and required outcomes, there is the continuing need to differentiate what an entity can do to reduce likelihood of malicious acts (which a combined PSO/ECSO can address) and plan for natural or accidental hazards that disrupt responsibilities which goes to more generic emergency , crisis and

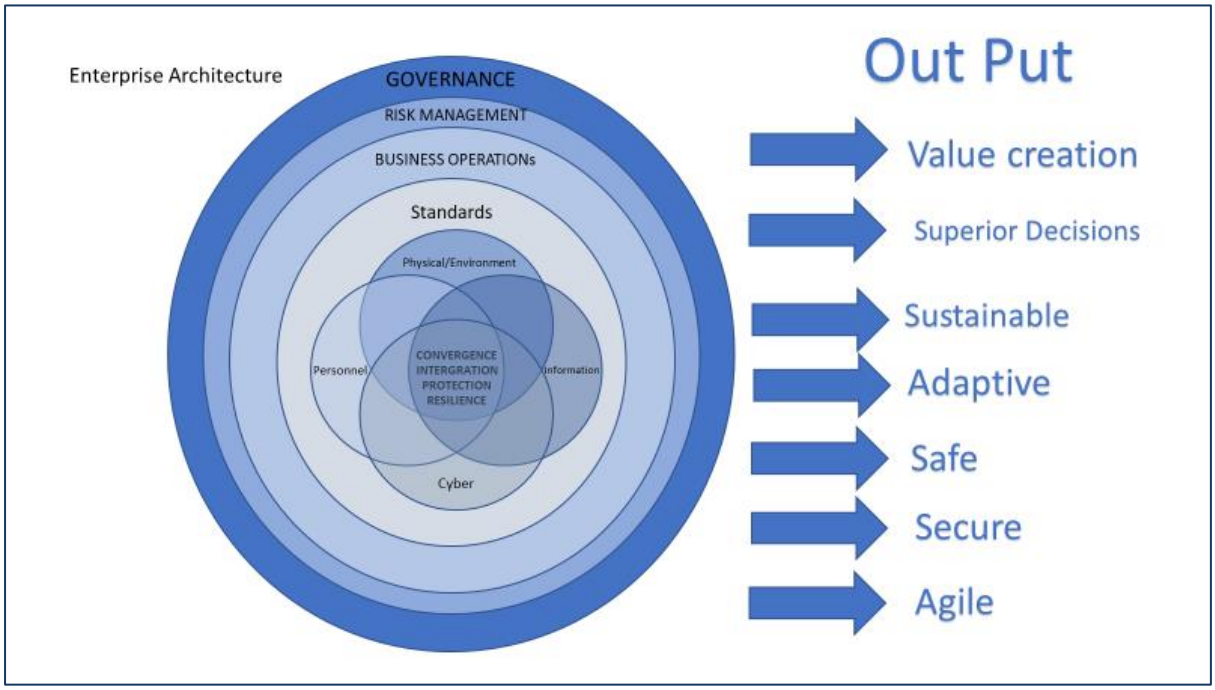
business continuity planning. Many FASE members have these responsibilities and we are happy to support these elements with relevant expertise

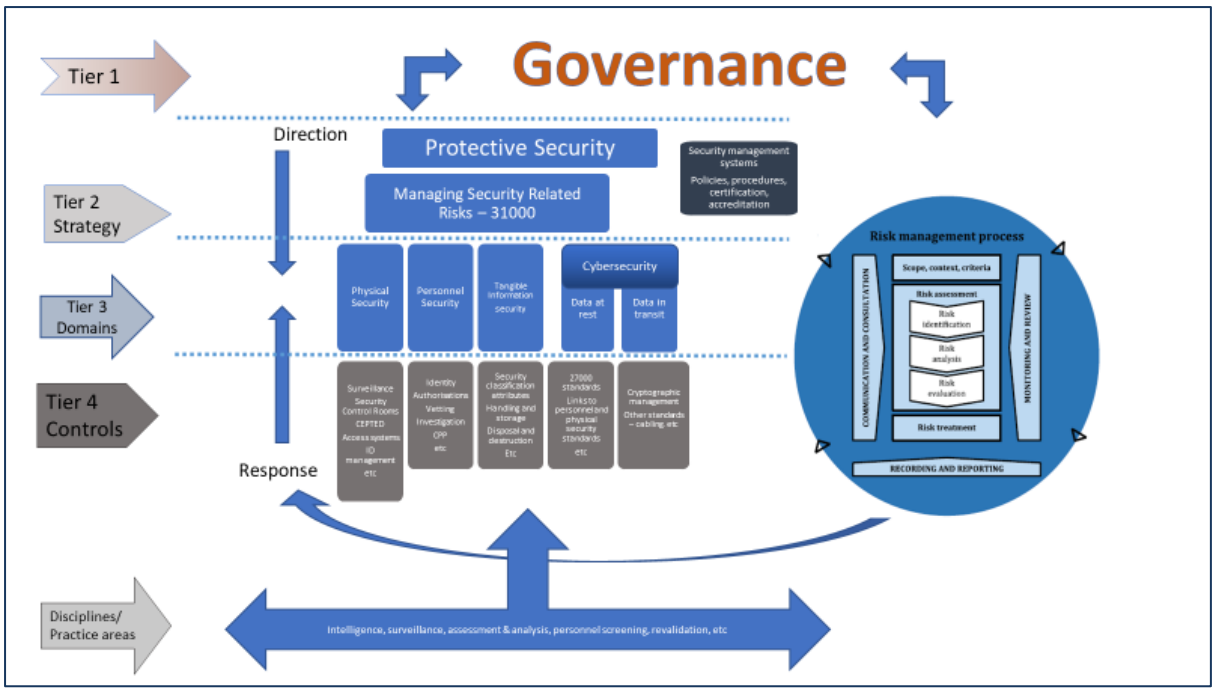
The primary issue is the requirement to have a co-design and development of the regulatory framework. It is disappointing that insufficient time is available for detailed study of the legislative amendments and analysis of potential consequences for regulation and implementation. This can be contrasted to the co-design of the Defence Trade Control legislation which was co-designed with industry, multiple departmental and academic representatives at senior level, and therefrom avoided many unintentional consequences and provided a world class legislation.

FASE is ready to provide both general and specific professional advice on a range of resilience, crisis and emergency management, protective security (including Cyber) and enterprise risk management.

It is noted that the new SOCI additions while specifically referencing Physical, Cyber, Personnel (omitting information in tangible form) apparently covered under Cyber) and Supply Chain security is logically inconsistent. We suggest that Supply Chain Security is actually the application of security controls to the supply function rather that a domain of control. Security of the Supply Chain is an outcome of the other practices for which an entity can be held responsible. It is no difference to applying physical, personal, information and cyber requirements to ensure activities of people are secure.

Two possible Conceptual Models for developing and implementing a framework design are below;





FASE has a very diverse nature of the companies providing representatives to FASE that we as a Forum, seek better clarification on the designation of critical infrastructure assets and systems of national significance than is current. There does appear to an absence of clear criteria or examples within the Bill, leaving entities such as a significant number of members, without a baseline understanding of their potential obligations because we don't know whether we are included in their definition of Critical Infrastructure or own assets that they say are represented.

As the forum of non-government senior security leaders, FASE looks to maintaining an ongoing role in the development of enhanced CI protection, sustainment and resilience and looks forward to feedback on this submission and an ongoing dialogue.

FASE National Executive