Samuel Grunhard
First Assistant Secretary
Critical Infrastructure Security Division
Department of Home Affairs
Email: ci.reforms@homeaffairs.gov.au

27 November 2020

RE: Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020

Dear Mr Grunhard,

Thank you for the opportunity to provide a response to the Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill), and for continued engagement with Engineers Australia to assist the Department of Home Affairs in enhancing protection of Australia's critical infrastructure.

Engineers Australia is the peak member-based professional association for the engineering profession in Australia. With about 100,000 individual members across Australia, Engineers Australia represents individuals from a wide range of disciplines and branches of engineering. Established in 1919, the organisation is constituted by Royal Charter to advance the science and practice of engineering for the benefit of the community.

This submission has been informed by the Systems Engineering Society of Australia (SESA). SESA is a Technical Society of Engineers Australia and the Australian affiliated chapter of the International Council on Systems Engineering (INCOSE).

Whilst it is understood that the Bill will only form part of the policy protection which will be applied to our national critical infrastructure, the Bill defines new critical infrastructure sectors and new assets within those sectors and will ultimately have significant influence on the critical infrastructure risk management framework.

Engineers Australia is broadly supportive of the content of the Bill. However, consideration must be given to the interdependency between critical infrastructure assets, and the sociotechnical/human elements that comprise the broader systems encompassing these assets. Identifying the extensive capability systems that include and supplement assets will help to identify risks and vulnerabilities associated with those critical infrastructure assets to continue to perform their intended functions indefinitely.

A series of observations, associated concerns and recommendations for your consideration are enclosed.

Engineers Australia would welcome the opportunity to discuss this submission in more detail and please contact me on (02) 6270 6565 or JRussell@engineersaustralia.org.au if you require any further information.

Yours faithfully,

Jonathan Russell
General Manager, Policy and Advocacy
Engineers Australia

Critical Infrastructure Asset Types (Schedule 1 Part 1 Section 7)

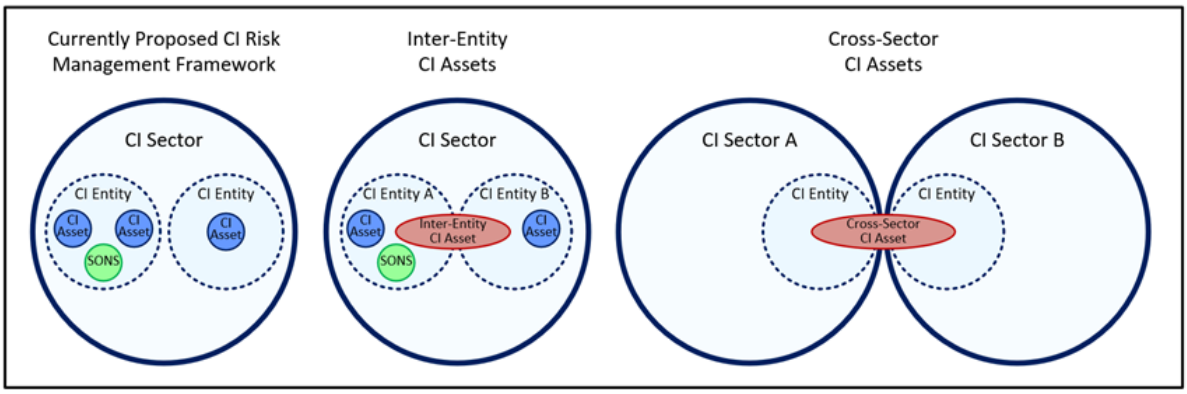
Observation

- Critical infrastructure entities have an obligation to produce an annual Critical Infrastructure Risk Management Program (RMP) identifying hazards (including cyber security incidents) and the *relevant impact* on their critical infrastructure asset.
- The bill focuses on cyber security incidents.
- There is an obligation on the critical infrastructure entity to comply with their critical infrastructure RMP and to minimise the likelihood of the hazards occurring (though no detail as to how this is assessed).

Concern

- All critical infrastructure asset types are defined under each critical infrastructure sector, which suggests there may be critical infrastructure asset types that have been missed, such as cross-entity and cross sectoral asset types (for which there are multiple critical infrastructure entities). For example:

    a) the Australian Warning System (AWS) may not fall into a single critical infrastructure sector; and,
    b) the Australian Tsunami Warning System (ATWS) is comprised of elements owned by three different agencies (Geoscience Australia, BOM and the Crisis Coordination Centre within DHA).



Recommendations

- Consider inclusion of critical infrastructure assets that fall within multiple critical infrastructure sectors (cross-sector critical infrastructure assets) and/or for which there are multiple critical infrastructure entities.
- Consider identification of essential services that can be mapped to all the contributing assets and/or entities that enable that service. This could assist in identification of critical infrastructure assets that may otherwise be missed.

Downstream Impacts (Schedule 1 Part 1 Section 21)

Observation

- The definition of *relevant impact* under section 8G, limits the impact of a hazard, and/or cyber security incidents to the impact on the critical infrastructure asset itself, ignoring impacts on other critical infrastructure assets.

Concern

- While the bill is cognisant of the potential for a *domino effect that degrades or disrupts others*, it is agnostic to this cascading effect within the critical infrastructure RMP.

Recommendation

- Consideration of mandatory capture of the potential scale of downstream effects within the critical infrastructure RMP (for example, the approximate number of business and/or retail customers served by the critical infrastructure asset) is recommended.

Time Domain (Schedule 1 Part 1 Section Part 39)

Observation

- The definition of critical infrastructure refers to infrastructure that might be *destroyed, degraded or rendered unavailable for an extended period*. While it does not specify the timeframe of an *extended period*, this is implied to be a long time.

Concern

- The loss of a critical infrastructure asset may not *significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security* until after a period has elapsed. For example, the defence industry may have sufficient stock to maintain supply for some time after the degradation or destruction of the critical infrastructure occurred.
- A cyber security incident may render a critical infrastructure asset temporarily unavailable. However, it may also be used to affect permanent/physical damage to a critical infrastructure asset. In the latter case, the impact may extend far beyond the incident itself. For example, the Esso Longford gas explosion in Victoria in 1998 resulted in the loss of gas supply to Victoria for 2 weeks, with broad reaching consequences, including to the hospitality industry and residential hot-water, heating and cooking.

Recommendation

- Critical infrastructure entities should be required to quantify the amount of time the critical infrastructure asset can be unavailable before the impact reaches the threshold of *significant impact* (maximum acceptable outage duration) in the critical infrastructure RMP.
- Critical infrastructure entities should be required to estimate the potential duration of the impact of hazards and cyber security incidents (expected outage duration or Mean Time to Restore (MTTR)) in the critical infrastructure RMP.

Hazards other than Cyber Security Incidents (Schedule 1 Part 1 Section 21)

Observation

- The positive security obligations focus almost entirely on cyber security incidents, notwithstanding the term *hazard* being used generically, and the critical infrastructure RMP covering hazards as well as cyber security incidents.

Concern

- While cyber security incidents are undeniably a growing threat, and one that can potentially be carried out remotely, security is broader than just cyber security. There is a lack of emphasis on a) malicious b) negligent c) accidental and d) natural threats.

These threats can all be identified and addressed proactively. For example: the Fukushima Daiichi nuclear disaster in 2011 was caused by an earthquake (and the resulting tsunami) that a) triggered the automatic shutdown of the nuclear power plant and the starting of the emergency diesel generators; and, b) the failure of those diesel generators due to the insufficient tsunami protection afforded to them.

Recommendation

- In addition to cyber security threats, increased emphasis must be placed on other type of hazards that should be captured in the critical infrastructure RMP.

Other Reports that may Inform the Bill

Observation

- The *Royal Commission into National Natural Disaster Arrangements – Report* (28 Oct 2020) was recently released.
- Engineers Australia produced the *Industry Responses in a Collapse of Global Governance* report as part of a collaboration effort with the Department of Defence in February 2019.

Concern

- Whilst the timing of the release of the Royal Commission report overlaps with the development of the Bill, the report contains several recommendations that are relevant to the protection and security of critical infrastructure.
- The *Industry Responses in a Collapse of Global Governance* report provides insight into some of the national risks to consider in the event of a major disruption to the global supply chain. This report focuses on the ongoing availability of supplies that are ordinarily considered as critical infrastructure assets but could have significant impact on critical infrastructure assets.

Recommendations

- Consult the *Royal Commission into National Natural Disaster Arrangements - Report* recommendations to inform the bill.
- Consult the *Industry Responses in a Collapse of Global Governance* report to inform the bill.[1]

Definition of Critical Infrastructure Risk Management Program (Schedule 1 Part 1 Section 2)

Observation

- Subsection 4(1) proposes the addition that the critical infrastructure risk management program *has the same meaning as in the Security of Critical Infrastructure Act 2018.*

Concern

- Security of Critical Infrastructure Act 2018 does not appear to define *Critical Infrastructure Risk Management Program*.

Recommendation

- Provide a definition of critical infrastructure risk management program that is consistent with external reference documents.

[1] A copy of the report is available at https://www.engineersaustralia.org.au/sites/default/files/resource-files/2020-05/Industry%20Mobilisation%20-%20Engineers%20Australia%20workshop%20report.pdf