7 December 2020

Department of Home Affairs
Critical Infrastructure Centre

By email: ci.reforms@homeaffairs.gov.au

## Protecting Critical Infrastructure Draft Bill

The Financial Services Council (**FSC**) thanks the Department of Home Affairs (**The Department**) for the opportunity to provide a submission on a draft of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*, accompanied by an Explanatory Document (**the Draft Legislation**).

## About the Financial Services Council

The FSC is a leading peak body which sets mandatory Standards and develops policy for more than 100 member companies in Australia's largest industry sector, financial services. Our Full Members represent Australia's retail and wholesale funds management businesses, superannuation funds, life insurers, financial advisory networks and licensed trustee companies. Our Supporting Members represent the professional services firms such as ICT, consulting, accounting, legal, recruitment, actuarial and research houses.

The financial services industry is responsible for investing $3 trillion on behalf of more than 15.6 million Australians. The pool of funds under management is larger than Australia's GDP and the capitalisation of the Australian Securities Exchange and is the fourth largest pool of managed funds in the world.

## FSC response to the Draft Legislation

The FSC notes that the Draft Legislation has a broader reach than was anticipated from the initial consultation paper. It appears that the Draft will result in another regulatory agency being imposed on financial services without a requirement for a streamlined approach with other agencies that already operate in financial services, including FIRB, ASIC, APRA, RBA and to some extent the Australian Information Commissioner.

Noting Australia's national savings system is robustly regulated, the FSC submits that there is potential for the proposals to duplicate, at unnecessary cost, a range of existing systems, particularly APRA prudential standards.

Given this, the FSC supports the approach outlined in the EM for Government to work 'with responsible entities of critical infrastructure assets to ensure the new requirements build on and do not duplicate existing regulatory frameworks.'

To deliver on this commitment, the FSC submits that the Department should work with the Council of Financial Regulators to ensure the reforms maximise the use of existing regulatory frameworks that monitor and govern the financial services sector's approach to risk management, information security, business continuity and outsourcing. The commitment in paragraph 25 and 26 of the EM implies that the proposals will be implemented using existing regulators, although this is not clear – the FSC requests that this be clarified in explanatory materials or regulations.


**Financial Services Council Ltd**
Level 24, 44 Market St
Sydney NSW 2000
E. info@fsc.org.au
W. fsc.org.au
ABN 82 080 744 163
@FinServCouncil
@FinServCouncil
@financial-services-council

We also submit that the proposals should align various security obligations with APRA's prudential standards, including:

- CPS 220 *Risk Management*;
- CPS 234 *Information Security*;
- CPS 232 *Business Continuity*; and
- CPS 231 *Outsourcing*.

The FSC draws particular attention to CPS 234 which has been adopted as the cyber security benchmark among prudentially regulated entities (which include life insurers and superannuation funds). Prudentially regulated entities have taken significant steps in the last year to work with APRA on this issue. Under CPS 234, boards of prudentially regulated entities have become formally accountable for cyber security; the FSC submits that this has resulted in appropriate levels of visibility, funding, and support to enhance Australian cyber resilience.

The FSC therefore submits that should these obligations be imposed ('switched on'):

- with respect to the Positive Security Obligation, where information on serious cyber security incidents is already reported to another government agency (eg, reporting to APRA under CPS 234), ACSC should look to obtain this information from that government agency to avoid imposing duplicate reporting obligations on RSEs
- with respect to critical infrastructure risk management programs, the new requirements should not duplicate obligations under CPS 234 and where possible, government agencies should seek to share information to ensure duplicate reporting obligations are not imposed on RSEs

We understand the proposals are expected to be finalised early in 2021 and to take effect from 1 July 2021. The Minister would need to make a decision to impose the relevant obligations (s81A, 30AB and 30BB). We request that the Department and Minister commit to providing adequate consultation and timeframes for any decision to impose the obligations. Implementing change with inadequate timeframe would be challenging in any circumstances however will be more so considering the volume of existing financial services changes being implemented in 2021, including numerous changes in response to the Financial Services Royal Commission, the Design and Distribution Obligations, and the Your Future Your Super reforms.

## Detailed comments

In our previous submission,[1] the FSC questioned whether smaller financial services businesses, fund managers or advice practices etc should be captured as "critical infrastructure entities and systems". This issue still remains with the Draft Legislation.

The FSC requests clarification for asset owners (including superannuation funds and fund managers) about whether it is the owning entity or the operating entity that attracts the obligations under the Draft Legislation. It is likely that asset owners will own assets that are on the critical asset list, and may be regulated critical infrastructure or even systems of national significance.

The FSC submits it is important that it is clear whether it is the owning or the operating entity that has the obligations. The Draft Legislation introduces the term "responsible entity". We understand this is meant to mean the entity with operational control over an asset, the FSC requests further clarity on this issue.

[1] Available from: https://fsc.org.au/resources/2100-fsc-submission-protecting-critical-infrastructure-consultation/file

The Draft Legislation proposes the responsible entity for a critical superannuation asset will be an RSE under the SIS Act or any other entity prescribed by the rules in relation to the asset. We request further information on which entities that are not RSEs may be prescribed as the responsible entity for a critical super asset.

- It appears there may be an error in the EM. Clause 118 of the EM indicates that, 'RSEs have been identified as responsible entities as they would be the authorised operators of critical banking assets, and, as such, ultimately responsible for these asset's continued operation.' We assume this is intended to refer to 'critical superannuation asset' rather than 'critical banking assets' – this should be clarified.

The FSC submits that the timeframes for a cyber-security incident should be made consistent with CPS 234, provided that the definition of a 'cyber security incident' under the Draft Legislation presents a subset of the types of notifiable incidents under the definition of 'cyber security incident' under CPS 234. We submit that, in order to ensure consistency, the Draft Legislation should be revised from 24 hours to 72 hours from the time of becoming aware of a confirmed incident. We note that it is also critical to clearly distinguish between 'events' and 'incidents', which are clearly different and have different levels of practicability in respect of notification. To ensure consistency with existing regulation, the notification obligation should be confined to material incidents, with a clear definition provided.

We also note the Draft Legislation has significant interactions with the current changes to FIRB, and may be broad enough to expand the list/scope of listed companies that are captured under the FIRB reforms.

## Concluding comments

The FSC would be happy to discuss this submission further – please contact my assistant Regina McCulla on [redacted] or [redacted].

Yours sincerely

[redacted]

Sally Loane
Chief Executive