12 February 2021

Senator James Paterson
Chair, Parliamentary Joint Committee on Intelligence and Security
Parliament House
Canberra ACT 2600

Re: *Security Legislation Amendment (Critical Infrastructure) Bill 2020*

Dear Senator Paterson,

The Financial Services Council (FSC) thanks the Parliamentary Joint Committee on Intelligence and Security for the opportunity to provide a submission on the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*.

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 Bill

Avoiding Duplication

We wish to highlight a few key points previously raised in our submission on the exposure draft of this legislation.[1]

The FSC welcomes the commitment in the Explanatory Document that, *'The Government will continue to work with industry…to make sure that existing regulations, frameworks and guidelines are leveraged, and to minimise any duplication or unnecessary cost burden. Close co-design will be integral to understanding the most effective way to implement the proposed reforms, and ensure the impost to industry is well understood and balanced against Government's policy objectives to uplift critical infrastructure resilience and security against all hazards.'*

[1] Our previous submission can be found here https://fsc.org.au/resources-category/submission/2127-fsc-submission-protecting-critical-infrastructure-draft-bill/file

Financial Services Council Ltd
Level 5, 16 Spring Street
Sydney NSW 2000
E. info@fsc.org.au
W. fsc.org.au
ABN 82 080 744 163
@FinServCouncil
@FinServCouncil
@financial-services-council

As we have previously submitted, this Bill imposes additional requirements on the already highly regulated financial services sector. It results in another regulatory agency overseeing financial services. Australian Prudential Regulation Authority (APRA) and Australian Securities and Investments Commission (ASIC) regulation already covers risk management, cyber security, data security and IT management.

The FSC submits that duplication with existing regulation and regulatory activities should be avoided, particularly with APRA prudential standards. We agree with the approach in the Explanatory Memorandum that the Government should *'work in partnership with responsible entities of critical infrastructure assets to ensure the new requirements build on and do not duplicate existing regulatory frameworks'* (at EM para 8).

The Positive Security Obligation

In 'switching on' and applying the positive security obligation, there should be a streamlined approach with other existing financial services regulators. The Department of Home Affairs should work with the Council of Financial Regulators to ensure the reforms complement existing regulatory frameworks that monitor and govern the financial services sector's approach to risk management, information security, business continuity and outsourcing.

Where information on serious cyber security incidents is already reported to another government agency (eg, reporting to APRA under CPS 234), the Australian Signals Directorate/Australian Cyber Security Centre should look to obtain this information from that government agency to avoid imposing duplicate reporting obligations on registerable superannuation entities (RSEs). Financial services organisations would not generally expect to be compelled to notify ASIC about a breach that has been reported to APRA as per section 912D of the *Corporations Act 2001* (Cth). That is, an AFSL holder is deemed to have reported the breach to ASIC if lodged with APRA. A similar principle should apply regarding notification to the Australian Signals Directorate/Australian Cyber Security Centre.

Similarly, IT security and cyber security issues may be the root cause, combined with human error, of a notifiable data breach to the Office of the Australian Information Commissioner (OAIC) under section 26 of the *Privacy Act 1988* (Cth). Financial services organisations reporting a privacy or data breach to the OAIC, which meets the eligibility criteria for notifying the privacy regulator, would not ordinarily expect to also be compelled to report the breach to other Government agencies unless specifically required to do so under relevant laws and regulations. Rather, they would expect that the OAIC would notify other Government agencies such as the Australian Signals Directorate/Australian Cyber Security Centre where they consider it relevant to do so.

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.

Proposed obligations 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.

In particular, CPS 234 has been adopted as the cyber security benchmark among prudentially regulated entities including life insurers and superannuation funds. 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.

Timing of the Bill and Regulations

We note that the commencement date will be a date set by Proclamation or 6 months after Royal Assent. This may not provide sufficient time to implement any required changes, especially considering the volume of financial services regulatory reform already underway in 2021 including the Financial Services Royal Commission, the Design and Distribution Obligations and the Your Future Your Super reforms. We submit that the Department and Minister should provide adequate consultation and timeframes for any decision to impose the obligations, at least 9-12 months after Royal Assent.

Other comments

The FSC submits that smaller financial services businesses, fund managers or advice practices should not be captured as 'critical infrastructure entities and systems'. The Government has not made a case that a small business in our industry with a limited number of clients and invested funds should be classified as "critical".

The Bill should clarify for asset owners (including superannuation funds and fund managers) whether it is the owning entity or the operating entity that attracts the obligations under the Draft Legislation. The Bill introduces the term "responsible entity". While we understand this to mean the entity with operational control over an asset, the FSC requests further clarity on this issue. 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 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 superannuation asset.

The FSC would also welcome more clarity around the threshold for a critical insurance asset. We would encourage the Government to consult broadly with industry and financial services regulators on what the appropriate threshold should be.

Concluding comments

The FSC would be happy to discuss this submission further – please contact [redacted]

Yours sincerely,

Chaneg Torres
Policy Manager, Investments & Global Markets