



27 November 2020

Department of Home Affairs
Critical Infrastructure Centre

[REDACTED]
[REDACTED]

By upload.

Dear Sir/Madam

**Re: AFMA response to Exposure Draft of the Security Legislation Amendment
(Critical Infrastructure) Bill 2020**

The Australian Financial Markets Association (AFMA) welcomes the invitation to provide comment to the Department of Home Affairs on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 ('the Bill'). AFMA appreciates the Department's consistent engagement and appropriate consultation process with the industry surrounding these reforms and hopes to keep up such meaningful collaboration going forward.

In this submission, AFMA raises a few outstanding concerns from the previous consultation.

Definition of Financial Services and Markets

While AFMA supports the definition of financial services and markets sector at the high level, we highlight the potential implications that arise with respect to the expanded definitions of 'critical infrastructure sector' and 'critical infrastructure asset' and the interaction with the current definition of 'direct interest holder' and the money lenders exemption in the *Security of Critical Infrastructure Act 2018 (Cth)*, 'SOCI Act'.

Definition of 'Direct Interest Holder' and Moneylender Exemption – s 8 of SOCI Act

- The significant expansion of the definition of 'critical infrastructure sector' and in turn 'critical infrastructure asset' under the Bill widens the scope of sectors and assets that are now subject to the requirements of the SOCI Act. The expansion of the proposed definitions is expected to result in financiers being captured as 'direct interest holders' under s 8 of the SOCI Act by virtue of taking a security position in assets that now fall within the scope of this Bill. In the event that a financier is captured as a direct Interest holder under the SOCI Act they would be subject to the reporting requirements with respect to the Register of Critical Infrastructure and in turn the civil penalties for non-compliance.

- We submit that banks and other lenders should be excluded from the definition of 'direct interest holder', to the effect that the moneylender exemption under s 8(2) of the SOCI Act would be amended to exclude financiers from the definition of 'direct interest holder'. The current moneylender exemption is largely inoperable, as it will only exclude a moneylender where the financier is not in a position to directly or indirectly influence or control the asset which is at odds with the purpose of enforcing against the security.

Additionally, we note the potential complications that may arise from the recent proposals in relation to amendments to Australia's foreign investment laws including the draft Foreign Investment Reform (Protecting Australia's National Security) Regulations 2020 and the Takeovers Fees Imposition Regulations 2020. We reiterate a particular concern for financiers, that under the draft amendments the business of the holding (and buying and selling) by a financier of debt secured over critical infrastructure will itself be a 'national security business'. This is an unintended consequence of the drafting of the moneylenders exemption in the SOCI Act, which may result in more transactions requiring approval from the Foreign Investment Review Board where syndicated lending arrangements between Australian and off-shore financiers are involved.

These concerns have been previously highlighted in submissions made by AFMA in relation to the exposure drafts of the Foreign Investment Reform (Protecting Australia's National Security) Regulations 2020 and the Takeovers Fees Imposition Regulations 2020.

Scoping of the Positive Security Obligation

AFMA welcomes the rationalised approach in the draft bill for the definition and scoping of 'responsible entities' in the financial services and markets sector. The proposed scope reflects an appreciation of the sophisticated technological maturities and cyber resilience frameworks implemented by financial institutions. Further, it also acknowledges the existing regulatory frameworks that address cyber security matters in the sector.

AFMA supports the suggested threshold for capturing entities subject to Positive Security Obligation (PSO) to be limited to banking entities with total assets above \$50 billion total, we view this as maintaining an appropriate focus on the most critical banking businesses.

AFMA also welcomes the indication by the government that the ministerial 'on switch' to activate the rules applicable to the three aspects of the PSO for a critical infrastructure asset or class of critical infrastructure assets, may be kept 'off' for APRA regulated entities, given the maturity and sophistication of the existing APRA arrangements and industry implementation.

Regulatory Harmonisation

AFMA notes the provision for leveraging existing regulatory frameworks wherever possible to administer the regime for critical infrastructure assets in the financial services and markets sector. We support a full consideration of such existing mechanisms and their implications in the codesign process of sector-specific obligations. AFMA appreciates the expressed commitment by the government to work with industry.

We note again our concerns that there are already multiple inconsistent standards with separate regulators in the financial services sector. We invite Home Affairs to consider

how these might be rationalised in the future, as an inconsistent approach administered by multiple regulators is unlikely to produce the desired security outcomes.

Ministerial Direction

AFMA notes the need to ensure that ministerial directions to entities and authorisations provided to the Secretary should be clearly defined and appropriately restrained. The government should take due account of the risks of the extensive intervention power. While the Bill creates provisions that would trigger ministerial action, such as being satisfied that an entity is unwilling or unable to respond to an incident or that no existing regulatory system could be used to provide an effective response to the incident, it is important to install robust checks and balances that necessitate clear evidential grounds for such satisfaction. Further, this intervention should be well-calibrated and aim to not disrupt the business environment.

AFMA reiterates that while firms should be required to take reasonable steps to prevent cyber-attack, the failure of these steps for victims of cyber-attack should not be sufficient for agencies to take a default view that the steps taken were not reasonable.

AFMA supports that ministerial intervention, when justly warranted, should not lead to a regulatory trend that reflects distrust in the industry's capacity. The government should uphold an educative regulatory approach that promotes market efficiency, resilience and integrity, instead of relying on a punitive regulatory model that risks harming the business environment.

Effective Information Sharing

AFMA supports a consistent government-industry collaboration and an industry-wide information sharing network. We note that the financial services industry already shares a disproportionately large amount of cyber intelligence with the government through existing regulatory and information sharing frameworks.

In contrast we understand that current government processes may retain much of the information and cyber intelligence that might be of benefit in a classified format, preventing it adding value back to the industry. AFMA supports exploring ways to facilitate increased prompt declassification and information sharing back with the industry.

Commercially sensitive information protection

While a reasonable and useful share of general information is beneficial for the ecosystem, AFMA notes the importance of ensuring confidentiality of entity-based commercially sensitive information that is provided to the government and regulatory agencies as part of legal and compliance obligations. AFMA notes that given the information sharing obligations introduced by the Bill, it is imperative to uphold the legitimacy of the regulatory data collection regime.

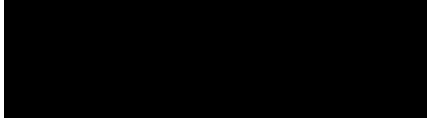
We note the approach the Government has taken in the Consumer Data Right which gives individuals and firms rights as 'data subjects' over their data. This approach is more aligned with seeing the data collected from firms as being held in trust for the benefit of the data subject and the purposes for which it was collected.

We suggest the government should similarly see the data it holds from firms as not being its own data but the data of the entities it regulates held in trust for regulatory purposes.

This particularly refers to access to 'system information' authorised by ministerial direction proposed by the bill. AFMA recommends the government to undertake an assessment of how the Bill interacts with the existing data collection legislation and regimes as well as the new proposed Data Availability and Transparency Bill.

AFMA looks forward to continued engagement and industry dialogue with the government to ensure an appropriate development of sector-specific rules. Please do not hesitate to contact Nikita Dhanraj on [REDACTED] or [REDACTED] if you need further information.

Yours sincerely

A large black rectangular redaction box covering the signature of the sender.

Damian Jeffree

Senior Director of Policy