16 September 2020

Department of Home Affairs
Critical Infrastructure Centre
3-5 National Circuit,
Barton ACT 2600

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

Dear Critical Infrastructure Centre Team,

Re: Protecting Critical Infrastructure and Systems of National Significance

The Australian Financial Markets Association (AFMA) welcomes the invitation to provide comment to the Department of Home Affairs on the proposed reforms around Protecting Critical Infrastructure and Systems of National Significance. AFMA's members are highly connected information businesses and as a result are deeply engaged with cyber security.

AFMA supports the purpose behind an enhanced critical infrastructure framework for the Banking and Finance sector to support sector resilience in the face of an ever-evolving cyber threat environment. AFMA has been increasingly focused on the challenges faced in relation to information technology and cyber security; and regularly collaborates with its members and regulators over related implications.

Our main concern is that there needs to be a rational whole-of-government approach to cyber-security and one that does not place additional cost recovery burdens on business. The current obligations and their regulatory framework are not consistent or logical or in some cases even clear. It is imperative that the Government takes this opportunity to rationalise the current arrangements.

It is unlikely that an anywhere near optimal approach can be achieved by having up to four regulators (ASIC, APRA, ACCC, and DHA) widely differing approaches applying four inconsistent partly overlapping and partly complementary standards to the same firms in the financial markets sector alone.

A review of the logic of current overlapping and inconsistent arrangements should be undertaken before this unsteady foundation is built upon further. Appending further gap-filling measures to be administered by a jumble of regulators using widely variant regulatory approaches is unlikely to achieve the Government's aims.

Existing regulations, requirements and industry standards should be adopted in the first instance and then rationalised.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

The experience in the Australian regulatory context is that attempts to implement a 'responsive regulation' paradigm within single regulators will be very likely to fail. This is due to the inherent conflicts of interest in a single body that is responsible for investigation, prosecution, policy setting and industry support. It is critical that these functions be put into separate entities to avoid the natural collapse of the 'responsive' model into a punitive regulatory stance. Over the long term this is the most important element to get right to avoid the damage to the economy the shift to punitive regulation can cause.

In AFMA's view, it is also incumbent on the Government to ensure that the enhanced framework promotes consistency between domestic and international best practices. The resultant regulation should not create duplicative reporting costs or inadvertently compel global businesses to fragment their technology systems, impeding competition and innovation. There is little benefit in starting from scratch when there are well developed systems and practices elsewhere that could be readily be adopted and adapted locally.

In this submission, AFMA draws attention to some high-level considerations that should underpin the development of legislation, guidance, standards and regulation around protecting critical infrastructure and systems of national significance in the banking and finance sector. Further, we also address some specific issues raised through the questions.

We trust our general comments and responses to specific questions are of assistance and look forward to an active collaboration in co-designing the sector-specific standards.

Please do not hesitate to contact Nikita Dhanraj on (02) 9776 7994 or ndhanraj@afma.com.au if you need further information.

Yours sincerely

Damian Jeffree

Senior Director of Policy

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

Harmonised approach to cyber security supervision

AFMA notes that cyber security, data protection and technological advancement are international issues requiring global solutions. Australia's Cyber Security Strategy 2020 notes -

> "Although this Strategy is an Australian Government initiative, the Australian Government recognises the essential role of state and territory governments, businesses, academia, international partners and the broader community in realising our vision…"

AFMA is of the view that the international partnerships are key to avoiding fragmentation which could create additional cost barriers to the flow of global capital and its contribution to economic growth.

Several single jurisdictions and multilateral organisations have published documentation that are worth due consideration where extensions to current requirements are contemplated. The International Standards Organisation (ISO) has Information Security Standard 27001 (adopted locally as AS ISO/IEC 27001:2015). The World Bank publishes a periodically updated compilation of significant documents on cyber security for the financial sector[1]. High level principles for cyber security by organisations like G7 that cover cyber risk assessment and third-party cyber risk management can also serve as a useful starting point for globally consistent standards.

Perhaps most significant is the potential to work in with our major security partners to have commonality in the deployed systems and standards. The US in particular is the technological leader and has advanced standards some of which may be appropriate to leverage such as NIST. The FSB Lexicon (2018) supports cross-sectoral common understanding of cyber security and cyber resilience terminology.

Industry Mapping

AFMA suggests considering international initiatives for mapping important business services such as the UK's FCA consultation on building operational resilience by setting impact tolerances for important business services (i.e. thresholds for maximum tolerable disruption[2]). The paper notes that not all business services are important and only the important ones should be mapped. It further recommends mapping exercises of important business services to be scaled according to the role, size and complexity of the firms offering those business services. Thus, less complex firms are likely to have simpler and fewer important business services to map. As corollary to our comments on determining national significance, this approach will help demarcate the small subset of entities considered to be 'the most important' to the nation, i.e. *Systems of National*

---

[1] Financial Sector's Cybersecurity: A Regulatory Digest, *Financial Sector Advisory Centre, World Bank Group,* May 2019. http://pubdocs.worldbank.org/en/208271558450284768/CybersecDigest-3rd-Edition-May2019.pdf.

[2] Building operational resilience: impact tolerances for important business services and feedback to DP18/04, *Financial Conduct Authority.* https://www.fca.org.uk/publication/consultation/cp19-32.pdf

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

Significance (SoNS) which will additionally be subject to the Enhanced Cyber Security Obligations. Appropriate identification and mapping of 'important business service' and consequent designation of SoNS will allow for an efficient mapping process that is not unnecessarily resource intensive.

The mapping should be used effectively and need not be a one-off exercise. The process and frequency for updating mappings will need to be developed and evolved as more experience is gained.

A staged implementation of legislation in this regard needs to be considered. Starting with a 'core' set of systemically important entities within the industry may be beneficial rather than being comprehensive from the beginning. APRA in this case adopts an assessment methodology[3] that draws on the Basel Committee's four key indicators of systemic importance: size, interconnectedness, substitutability and complexity.

Due consideration should be given to how service providers and third parties that the sector outsources critical processes and support activities to, will be impacted by the regulation. AFMA elaborates on this point in question 6.

Regulatory Approach

Risk-based capturing of critical infrastructure entities by regulatory obligations

The DHA should work with the entities to enable them to reach a 'minimum' benchmark for security robustness which can shift with the evolving nature of cyber threats. The specification of any 'aspirational' target through guidance should be continually adjusted for the changes in the threat environment and thereby would not be appropriate for mandating.

While far from perfect there are some lessons to be learnt from the Hong Kong model in relation to information systems[4]. This methodology incorporates the risk profile, which is ascertained by balancing the level of inherent risk with the quality of risk management systems in place by firms. Risk-based regulation is a dynamic and forward-looking approach, which provides the regulatory process with the necessary framework to factor the risk profile of an entity into its assessment. The adoption of a more risk-based framework allows the regulator to continue to deliver more consistent, higher-quality supervision as the sector develops and risk profiles of firms change in reaction to competitive forces.

---

[3] APRA framework for domestic systematically important banks, *APRA,* https://www.apra.gov.au/news-and-publications/apra-releases-framework-for-domestic-systemically-important-banks-australia

[4] Supervisory Policy Manual, Risk-based Supervisory Approach, *Hong Kong Monetary Authority.* https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-1.pdf

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

Costs to Industry

We appreciate that the DHA does not plan on an industry-funded regulatory model. We support this position and would strongly oppose any suggestion of the recovery of government costs from industry. There is a strong public good element to the national security outcomes sought by government and industry.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

Questions

1. *Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?*

AFMA is focussed on financial services and so will not comment on this question.

2. *Do you think the current definition of Critical Infrastructure is still fit for purpose?*

We are broadly supportive of the identification of critical infrastructure approach and for many physical types of infrastructure the definition would be entirely suitable. AFMA is concerned however that in relation to digital technologies the infrastructure that provides the function or service should not be pinned down through a registration scheme. For example, ASX is currently upgrading the CHESS settlement system from a traditional database system to a blockchain based service. A few years ago this innovative transition would have been difficult to imagine. The CHESS infrastructure potentially may have qualified but is now obsolete. Regulatory barriers should not be placed in the way of upgrading digital infrastructure. As such we recommend that for digitally provided services the focus is on the service or function rather than the particular infrastructure used to provide the service.

3. *Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?*

AFMA supports a risk-based approach of determining infrastructure criticality and systems of national significance. Where there are multiple competing providers, and it would be possible for providers to back each other up this should decrease the level of regulatory intensity. We note also that since consequences of failure cannot always be accurately predicted, the focus of the enhanced framework should be management of risks and factors that may lead to failures.

4. *What are the common threats you routinely prepare for and those you have faced/ experienced as a business?*

Financial services firms respond on a risk basis to threats and their potential impacts. This will typically direct more resources to preparing for cyber-attacks that have a high likelihood due to the ease with which they can be executed (e.g. denial of service attacks, sending phishing emails with malware etc) and those where the impact will be material (e.g. loss of a critical system). Responses normally include:

- Implementing controls to prevent the attack and isolate and mitigate its impact.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

- Contracting for services that can be provided in the event of attack. (e.g. support for customers who have had personal private details stolen or expert forensic support.)
- Documenting incident response process/plans, cyber incident playbooks and business recovery plans.
- Testing plans and playbooks.

5. *How should criticality be assessed to ensure the most important entities are covered by the framework?*

AFMA supports a risk-based approach to determining criticality that factors in the sectors maturity levels and controls to mitigate risks.

We note again one criterion that should be considered when determining whether a piece of infrastructure should be designated of national significance is the level of redundancy built into the wider national system as it relates to that individual piece.

The financial markets have established differing levels of requirements for resiliency in infrastructure based on the significance to national markets. For example, in an environment where there are many competing providers, such as is the case with regard to market participants (e.g. stockbrokers) and one may take over from the other. While security and resilience are still important for single participants there is less concern with ensuring the highest levels of redundancies in each provider as they effectively back each other up. Where there are single providers for nationally significant infrastructure such as payments, higher standards of resilience have been required.

A similar analysis might be of assistance across many of the fields in which the CIC is working. For example, there may be similar considerations given to the relative national significance of a power station, such as a baseload coal-fired unit versus widely distributed intermittent sources like windfarms, by whether it has other stations which may step in to replace it during high demand periods.

AFMA and its members are open to collaborating with DHA on mapping and evaluating criticality.

In addition to the firm-level information and cyber security obligations, APRA-regulated entities are governed by standards which also include extensive third party-related reporting obligations. AFMA reiterates the role of service providers and recommends a careful consideration of any negative externalities of placing high-cost requirements on service providers.

6. *Which entities would you expect to be owners and operators of systems of national significance?*

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

The term 'owner' of critical infrastructure assets or systems is currently not defined under the SOCI Act which uses the term 'direct interest holder'. Our concern is to what extent an 'owner', if defined along the same lines as 'direct interest holder', could be held liable for a failure to comply with the PSOs and subject to potential enforcement action. Please refer to our comments on the term 'operator' elsewhere in this submission.

There are also potential implications for institutions as a lender to other critical infrastructure assets/systems where the institution takes security over the asset/system for the loans.

The SOCI Act defines both 'operators' and 'direct interest holders'. The Act provides an exemption to moneylenders with respect to the definition of direct interest holders provided the moneylending agreement does not put the money lender in a position to directly influence or control the CI asset. This exemption is largely unusable given its present wording. As such, circumstances have arisen where an institution meets or has the potential to meet (upon default of the borrower) the definition of a direct interest holder. Given the potential implications for institutions should they find themselves in a position where they are subject to the PSOs by virtue of a moneylending arrangement, the Act should introduce appropriate checks and balances to avoid unwarranted capture of entities as owners of critical infrastructure assets and systems.

Due consideration should be given to how service providers and third parties that the sector outsources critical processes and support activities to, will be impacted by the regulation as 'operators'. Functional outsourcing helps institutions to remain competitive and efficient by mitigating high costs, they also add bespoke technological sophistication and risk management given their wide-ranging expertise. The risks of associated with importing these efficiencies are well-addressed in existing prudential frameworks by APRA. CPS 234 ensures that regulated entities conduct complete, consistent and appropriate due diligence of their outsourcing arrangements and comply with the related reporting obligations. We propose an approach below designed to avoid duplication of these requirements.

7. *How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?*

AFMA suggest that the TISN constitutes a one-stop source of comprehensive as well as targeted information exchange. The network should actively engage with the financial market participants domestically and internationally to support best practices of crisis preparedness, assessment, management and resolution. One of the key takeaways from the COVID-19 pandemic was the need for industry-wide coordination around BCP testing, best practices and operational resilience measures. AFMA played an important role for its members and facilitated crucial industry-regulator liaison during the pandemic and would be open to work with the government on an optimal design for the TISN.

8. What might this new TISN model look like, and what entities should be included?

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

AFMA is open to active collaboration with the DHA design an expanded model for the TISN.

9. *How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?*

At a high-level, the Government should consistently involve the industry in the legislation and standard-making process to help its own understanding of the sector's risk environment, risk management controls and systems, existing regulation and international best practices. It should adopt 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.

There is likely to be a significant burden on the third-party service providers and supply chain, who, on top of Service Level Agreement penalties drafted into contracts with customers and customer-enforced due diligence in accordance with CPS 234, could be subject to regulatory action as part of this proposal. AFMA supports minimization of such impact and is open to further discussions on how this best might be achieved.

10. *Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?*

AFMA supports a principles-based approach as appropriate for determining the *aims* of the program, but we note caution around designing obligations around outcomes. As noted above outcomes may not be achieved for a wide range of reasons including difficulties in countering measures by highly resourced and determined state-backed actors.

We caution again against defining failures in relation to these aims (identification and understanding risks, preventing incidents, minimising incidents and ensuring effective governance) as being appropriate for sanction. The UK model referenced above under *Industry Mapping* recognises that failures can happen, by setting impact tolerances for important business services (i.e. thresholds for maximum tolerable disruption). This model is intended to change the mindset away from traditional risk management towards accepting that disruption to business services is inevitable and needs to be managed actively. This does not limit a firm's responsibility for compliance but proposes a more rationalised approach to building resilience against failures.

Victims of cyber-attacks should be required to take reasonable steps but the failure of these steps should not be sufficient for agencies to take a default view that the steps taken were not reasonable. Prosecutions are done with the benefit of hindsight and most failings can be characterised as unreasonable from that vantage point. Firms that take reasonable measures should have a measure of comfort that unlike in other areas of

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

regulation they will not be immediately on the defensive if an advanced actor is able to penetrate their cyber defences.

Similarly:

- It is not always possible for a reasonable actor (or even a state actor) to identify all risks in advance, particularly in a landscape of evolving threats.
- While minimisation of impacts of realised impacts is an important aim, cyber-attacks are inherently complex and are difficult to respond to in a time-pressured environment, so minimisation can be difficult or even impossible to achieve (even for state actors including the Government).
- Compliance programs cannot *ensure* that identified risks are effectively managed, only that reasonable efforts to manage risks are being made.

11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

The security obligations are a reasonable start. However, as with the principles we note the necessity to cast them appropriately as outcomes that firms should take reasonable steps towards. Some obligations are phrased in this way – e.g. 'Endeavouring', 'Aiming', etc. while others are not. Obligations should not be phrased in such a way that any failing in outcome leads to a presumption that a regulation has been breached.

We note the assurances given on the intended style of implementation by DHA on this point. However, we also note that our experience has been repeatedly that as staff turnover in a regulator or government body the original nuances of intention are lost and what remains on the page is what informs current staff and the resulting actions of these bodies.

12. *Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?*

Yes, the sector is largely mature and already works within a comprehensive framework of principles of processes, risk management and controls directed by both effective commercial strategies and compliance requirements. We do note, however, that there are variances in sophistication that have been reported with greater maturity in large firms versus SMEs. See ASIC Report 651.

Firms are subject to a range of regulatory and reporting obligations that while mostly granular also factor in the ever-evolving threat environment in terms of technology-agnostic standards.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

However, we note that any new regime will have substantial implementation costs as firms seek to understand the new paradigm and take appropriate steps to ensure that their organisation is in accord with it.

13. What costs would organisations take on to meet these new obligations?

Firms will take on a range of new material costs in relation to the obligations. These include:

- A review of current arrangements and assessment against the new requirements;
- Remediation of any gaps identified;
- The design and implementation of new information sharing and reporting arrangements;
- Testing and review of the new arrangements;
- Participation costs for industry tests; and
- Extension of audit regimes to cover the new requirements.

14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

The financial services sector is subject to a range of security obligations. As noted above, global entities are subject to different security obligations and standards across national borders. The sector's maturity and focus on ensuring critical asset protection not just from a compliance perspective but also as one of the principal business objectives, is indicative of the significant resources that are already invested to achieve the most effective security goals.

We understand that the DHA has reached out to firms to engage in an independent economic modelling and cost-benefit analysis around the proposed framework. AFMA supports such independent, transparent and ongoing analyses with maximum industry engagement to inform any policy-making and standard-setting.

15. *Would the proposed regulatory model avoid duplication with existing oversight requirements?*

Current arrangements

AFMA has been an active participant in the development of cyber security regulations by the current regulators.

It is important that before DHA considers utilising this existing regulatory infrastructure as a foundation for further regulatory construction that it considers the current state of this regulation. In AFMA's view, if DHA were to implement the proposed program and include a reliance on the existing regulatory structures and infrastructure this would likely lead to:

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

- A further increase in complexity and duplication of requirements;
- Increased inconsistency of enforcement approach;
- Less reliable and more variable security outcomes; and
- Delays in uplift for sectors where regulators that use an effectively punitive approach to regulation.

The current arrangements of multiple competing and inconsistent requirements have come about from the competing and divergent interests and perspectives of the regulators.

These regulators bring a varied array of approaches to the task:

- APRA developed a sensible but unfortunately globally unique standard in CPS 234. This was complemented with finely grained guidance in CPG 234. The implementation timeframe was short however and firms faced a new complex set of compliance requirements with insufficient time allowed for full compliance with the guidance on release. APRA engaged constructively with industry to assist with the transition to the new standards and has not led with litigation (court-based enforcement actions).
- ASIC consulted on a *draft* approach to resilience and security in financial markets in CP 314 but has yet to release the finalised Market Integrity Rules associated with the consultation. It has commenced litigation recently against a firm for alleged breaches of licence obligations in relation to cyber security. ASIC has publicly committed to a 'why not litigate' approach to regulation that is unlikely be aligned with the responsive approach that has been suggested in the consultation as the proposed approach by DHA. Active litigation has previously limited ASIC's responsiveness to requests for greater guidance on regulatory matters.
- ACCC developed yet another set of standards in relation to the Consumer Data Right (CDR). The standards were influenced by, but different to, the APRA standard. Within the CDR AFMA argued for consistency of standards across all firms seeking to access the scheme to ensure there were not softer points of access for sensitive data. The final standard, however, persisted with variable requirements. Schedule 1 Part 2 of the relevant requirements allow a lower standard of security for non-ADI firms with access to the same sensitive 'read' data. ACCC utilises a punitive approach to regulatory enforcement which is not aligned with the responsive regulation approach described in the paper.

Of particular concern is that the litigation-driven punitive approaches to regulatory enforcement of a number of regulators are unlikely to deliver security improvements in a time-effective manner and are likely to lead to delays and uncertainty in delivering requirements. This is because litigation-based approaches are generally retrospective as they are driven by the findings and vagaries of court cases which typically take many years to play out.

If the Government priority is swiftly lifting the standards of information security and other security measures then this is far more likely to be achieved with an accommodative

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

approach to both the old and new requirements, and a rationalisation of current arrangements into a single national system for cyber and related security across all industries (with appropriately graduated standards within each).

Responsive Regulation in single bodies

The consultation paper suggests that DHA proposes to adopt a Responsive Regulation approach to the enforcement of security requirements. Responsive regulation was originally proposed by Braithwaite and Ayres in 1992 as a 'third way' between the accommodative and punitive regulatory approaches.

While it is beyond the scope of this submission to comprehensively review responsive regulation, AFMA has long observed that placing a responsive regulation paradigm within a single body creates conflicts that over time are very likely to move the body to a punitive approach. ASIC's recent crystallization of 'why not litigate' into a formal policy, for a nominally responsive body, is an example of this type of shift which has occurred over many years.

Regulators can be stable in a punitive regulatory mode, or an accommodative regulatory mode. However, attempts to have a variable mode within a single body face severe challenge to avoid a collapse towards a punitive setting. Effectively a single regulatory body is inherently unstable in any 'middle way' approach, including 'responsive regulation', as incentives for the body and its staff are strongly skewed towards more punitive outcomes.

It may be that these conflicts can only be managed effectively in more traditional structures where functions are separated into separate bodies such as:

- policy and rulemaking bodies (such as the Parliament and government departments);
- investigatory functions (such as by general policing bodies);
- decisions and actions to prosecute (such as through a general purpose DPP); and
- industry support bodies (such as the Australian Cyber Security Centre).

The combination of these functions into a single body creates a complex matrix of conflicts of interest that is fundamentally incompatible with a responsive regulation paradigm. The risks towards punitive outcomes of a single body being invested with these functions has long been known[5]. While strong leadership can resist these forces to some extent for some period, over time pressures from external reviews by bodies and individuals that understand and expect a punitive approach will continue.

An example of the conflicts inherent include that it is in the interests of the prosecutorial arm of a single body regulator to create rules and policies that are easy to prosecute, and to set the penalties very high to produce leverage over the accused. There are no

[5] See for example: https://books.google.com.au/books?id=ZjoIAAAAQAAJ&vq=%398&pg=PA398#v=onepage&q=398&f=false

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

countervailing pressures to preserve basic freedoms and rights. The Australian Law Reform Commission recently argued against the practice of regulators characterising a single offence in multiple ways (for example as a penalty matter, a civil offence, and a criminal offence) as being an inappropriate way of approaching justice.

Similarly, decisions to prosecute risk influence from the interest of the body in appearing 'tough' on an entity or a sector when these decisions should only be based on what is fair and reasonable. Even where prosecutions ultimately are likely to fail, as these defeats are long-delayed these risks can be heavily discounted.

Support functions, such as providing guidance as to safe harbours can be restricted in the interest of litigation that is on-foot and the prosecutorial interest in maximising the chances of success in court. There are many more such conflicts that are inherent in single-body responsive regulation.

As a result of these conflicts, responsive regulation as an instruction for a single body (typically a regulator) has in general terms resulted in regulatory stances, penalty schemes, and approaches to regulation that are punitive and are not supportive of the creation of an attractive business environment that can compete internationally and maximise beneficial economic activity domestically. At a high level they have contributed significantly to the rise in regulation that is not supportive of the national interest.

Cyber and national security in general are national interests that are too important in the current context to allow a fragmented and conflicted approach to persist in order to preserve existing regulatory divisions unaffected.

Proposed regulatory structure

AFMA proposes that cyber-security adopt a more traditional multi-body approach to its implementation and enforcement, but with single bodies responsible for each function across multiple industries. Existing arrangements and responsibilities would be folded into the structure over time.

This approach would bring consistency in policy approach, industry support, investigation and where required *in extremis* prosecution across all critical industries. This will ensure a timelier, integrated, cost-effective and strategic approach as opposed to a fragmentated outcome that would result from extension of existing unsatisfactory regulatory arrangements.

We suggest that:

- The policy making function be done within a relevant existing Government department such as DHA. Existing sectoral obligations could be picked up from the current regulators by DHA, initially as is, and then rationalised and made consistent over time across industries with consistent graduated levels based on international standards.
- The support from the Government to industry should be provided by ACSC. Reports of breaches should be given the ACSC to assist with keeping an accurate

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

national view of threats. There should be clear separation between reporting obligations and enforcement which should be done by other bodies. A failing of some regulators' current structures is that a lack of separation of policy from enforcement results in underinformed policy flowing from a reticence to report issues. The creation of incentives to minimise reporting should be avoided by this separation of function. A cooperative arrangement would maximise the intelligence available to ACSC.

- Where ACSC has issued a direction and the entity actively does not comply this could be referred to the Federal Police for enforcement and/or the DPP for potential prosecution. A clear separation in the structures should ensure that this is a significant step removed from the normal supportive functioning of the regulatory apparatus, and that self-reports are not used for prosecution.

Regulations must be designed so that prosecution is only a responsive to intentional or reckless failings.

AFMA has been on the record before in arguing against regulations that are framed such that they characterise all outages and operational imperfections as breaches of regulation.[6] Matters arising from self-reports should not, generally speaking, be treated as fundamental breaches of law that are appropriate for punishment. As to do so would be the equivalent of blaming the bank for a robbery. Similarly, the victims of cyber-attacks should not be blamed for being attacked by sophisticated potentially state-backed actors and failing to defeat the latest advances in cyber intrusion. Industry is there to assist preventing such issues and outcomes as it is in their self-interest.

The self-interest of all involved is the protection and preservation of proprietary data. No entity in the system wishes to have its data compromised from a commercial perspective. Nevertheless, the pace of technological change is so great that it challenges all involved, including the Government, to keep ahead of the rapidly escalating threat. The mere fact that a breach has occurred should not be the trigger for further detriment to the firm by the Government that purports to protect it and the wider economy. It is critical that the apparatus of government remains part of the solution rather than contributing further to the problem.

In order to secure positive collaboration a mutually supportive relationship needs to be basis for this system. The industry should be in a collaborative relationship with government and the regulatory arrangements must be carefully set up to ensure this paradigm. The interests of industry are convergent with those of government and should not create a relationship where industry is characterised as fundamental wrongdoers in failing to prevent attacks.

As such, ACSC should not be given the power to impose fines on firms. This would damage the relationship with industry and inhibit their ongoing cooperation beyond what is legally required. ASCS should be preserved as a positive and valued partner of industry.

[6] https://download.asic.gov.au/media/5355855/cp314-submission-afma.pdf

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

AUSTRAC provides a clear example of the type of regulatory outcome that would be highly damaging for the economy. AUSTRAC was set up as a data collection agency to assist law enforcement prevent crimes by money launderers and other criminals.

The industry was always keen to assist with the important work of aiding in the capture of those breaking money-laundering and other laws. Over time, however, the failure to achieve perfection in the data provided to assist with this important work, itself has become the most significant financial risk for financial services firms.

The failure to provide perfect data to assist government to prevent crime has effectively been conflated by regulators and others with the crimes the provision of data was designed to catch. This confused approach has been and continues to be highly damaging to the Australian business environment.

We are concerned that the proposed changes will extend this approach to other areas of regulation. If Australia were to become known as a jurisdiction where it was too risky from a regulatory perspective to set up a digitally connected enterprise due to the risk of AUSTRAC-style extreme fines then the regulatory system itself would be complicit in damaging the prospects for the economy. While a stepped and mostly supportive regime is the stated aim in the consultation paper, the proposed approach is, while no doubt well-intentioned, likely to result in damaging outcomes for the business environment. The current consultation provides an opportunity to set a different and more successful course for regulation in this important field.

16. *The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?*

AFMA supports early, extensive and empowered engagement with the industry to develop guidance. This involves including industry and other parties at the ideas stage before a proposal is prepared. An issues paper can assist in this purpose.

The project of providing our input for guidance, broader communication and engagement strategies is beyond the time available to respond to this consultation. However, AFMA would value the opportunity to be a part of this process over the course of the next 6 months.

17. *Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?*

Please see our answer to Question 15.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

18. *What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?*

Please see our answer to Question 15.

19. *How can Government better support critical infrastructure entities in managing their security risks?*

The Australian Cyber Security Centre provides high quality and important support to business. We see scope for the significant expansion of their industry engagement programs including wider coverage, more sector specific coordination and scenario testing.

20. *In the AusCheck scheme, potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?*

We would like to highlight that some banks already have arrangements for exchange of sensitive information with the Government. These arrangements should continue to be used.

We also highlight that banks have a range of existing processes for hires, including probity checks, background, financial and criminal checks. We would like to better understand the potential role of the AusCheck scheme in this context.

21. *Do you have any other comments you would like to make regarding the PSO?*

Not at this time.

22. *Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?*

Refer to our response to question 7, about considering threats on a dynamic basis.

23. *What information would you like to see shared with critical infrastructure by Government? What benefits would you expect from greater sharing?*

The 2020 Strategy identifies the need to increase information sharing, including the proposal for a new portal. The Australian Government could leverage the lessons learned from the FS-ISAC on private and private-public (CERES) efforts on information sharing.

Where the requirements for data/information/metrics are concerned, PII regulations may potentially conflict with the regulator's requests. The definition of critical asset should be

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

defined more specifically to the lens of the Australian economy. E.g. applicable systems containing data related to Australian business. This would assist in demarcating the legislative jurisdiction to what is most relevant.

24. *What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?*

Not applicable.

25. *What methods should be involved to identify vulnerabilities at the perimeter of critical networks?*

Not applicable.

26. *What are the barriers to owners and operators acting on information alerts from Government?*

Not applicable.

27. *What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?*

Having a consistent approach across sectoral 'playbooks' or frameworks can help to identify cross-sectoral risks and threats. We also refer to our response to question 24.

We note that banks receive information about risks and threats from commercial vendors. The terms of the commercial contract may constrain the information that banks can share or how information is shared.

28. *What safeguards or assurances would you expect to see for information provided to Government?*

We consider a number of safeguards and assurances are important. These include:

- Protection for information that can expose vulnerabilities in a bank's system or in a sector;
- Protection for commercial confidential information;
- Clear safeguards and restrictions on which government agencies can access the information;
- Clear restrictions on the use of such information preventing it being used in an investigation, or a regulatory or enforcement action.

We also note that to gather more information about incidents it is sometimes in the interests of parties under attack not to respond immediately. It is imperative that the

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

discretion to manage these type of decisions remains with the private sector as they are best placed within a liberal democracy and a market-based economy to make these decisions and are likely to be appropriately incentivised without top-down state interventions.

29. *In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?*

The starting working position should be that the great majority of firms can be expected to be working hard to prevent cyber-attacks and assist authorities in their response.

Direct action may be appropriate where it has been confirmed that either the firm is not taking reasonable steps (and there must be some allowance here for reasonable variance by the firm on what this should be) to assist with a directive or the firm invites the intervention to assist with its response.

AFMA supports clarity around how, when and to what extent would direct active assistance from the Government be warranted. Government should engage with industry to determine the optimal extent to which an organisation's decision-making process and its own interests are being overridden and how this conflict is managed. We propose that this highly unlikely possibility is dealt with in a rationalised, case-to-case basis without excessive prescriptive direction.

We restate that, firms in the financial services sector have sophisticated and well-developed infrastructure and processes in place to effectively counter threats that may emerge. Coordinating efforts in the event of an imminent or realised serious cyber incident would be critical to a proportionate and rapid response. Firms need to be connected to the right government support which is founded upon suitable competence and a deep understanding of the broader financial system.

30. *Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?*

Under our model the ACSC would be the body to make this call.

31. *Who should oversee the Government's use of these powers?*

There should be the opportunity for judicial review and a post-review by a third party that is independent of the ACSC.

32. *If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber-attack, do you think there should be different actions for attackers depending on their location?*

AFMA has no comment.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au

33. *What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?*

Consistent with our above framework industry officers working in good faith to prevent and respond to cyber-attacks should not be the target of prosecution.

If against this advice firms are exposed to a prosecutorial regime when working in good faith this should apply equally to government officers for similar failings.

34. *What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?*

These are significant powers and need a comprehensive framework of checks and balances. AFMA would be pleased to assist with the design of such a scheme.

35. *What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?*

No comment.

36. *Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?*

Subject to our comments above we are broadly supportive of the roles of government and industry as outlined. It is important to preserve the strengths of market based liberal democracies and avoid the costs of excessive regulatory intervention and control.

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7900 Email: secretariat@afma.com.au