9 March 2024

Hamish Hansford
Deputy Secretary
Cyber and Infrastructure Security
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616
Via email: cisgcomms@homeaffairs.gov.au

Dear Mr Hansford

RE: Australian Cyber Security Strategy: Legislative Reforms

The FSC welcomes the opportunity to contribute to the consultation on the proposed legislative reforms that give effect to the National Cybersecurity Strategy (**The Strategy**). The FSC is supportive of robust measures that enable organisations to better prepare and recover from cyber incidents, including the ability to share and/or receive time critical and contemporary information with other affected organisations.

The FSC wishes to highlight where there may be inconsistencies or doubling up of regulatory requirements, especially regarding APRA's new prudential standard CPS 230: Operational Resilience (**CPS230**).

About the Financial Services Council

The FSC is a peak body which sets mandatory Standards and develops policy for more than 100 member companies in one of Australia's largest industry sectors, financial services. Our Full Members represent Australia's retail and wholesale funds management businesses, superannuation funds, and financial advice licensees.

The financial services industry is responsible for investing more than $3 trillion on behalf of over 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 one of the largest pools of managed funds in the world.

Summary of Recommendations

1. All organisations should be required to report ransomware attacks in some way, but the reporting regime should reference existing industry regulatory frameworks to minimise the impacts on entities.
2. Ransomware reporting timeframes should, where practicable, align with existing reporting requirements but allow sufficient time for entities to manage the crisis of a ransomware attack without adding additional regulatory burden.
3. Enforcement frameworks for ransomware reporting should be aligned with existing regulatory enforcement approaches so there is not a double up of regulatory measures.

4. The Cyber Incident Review Board should have a terms of reference that focusses on understanding a cyber incident with a view to uplifting preventive measures and preparedness in the future through the provision of education and guidance, as opposed to an enforcement or regulatory function.
5. The Cyber Incident Review Board should have a clear and published framework to consider when determining whether to investigate a cyber incident.
6. The Cyber Incident Review Board membership comprise experienced persons with a strong understanding of cybersecurity and technology as well as rotating members with industry-specific knowledge from key industry sectors likely to be targeted by transnational and serious organised cybercriminals.
7. Whatever body or person is responsible for referring matters to the Cyber Incident Review Board, the decision-making framework and the decisions made should be clear, transparent, and published.
8. Government should defer its remedy and review power to an appropriate regulator, such as APRA, where appropriate.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses.

Question 10: Which entities should be subject to the mandatory ransomware reporting obligations?

The FSC submits that it would be ideal to have mandatory ransomware reporting extended to all organisations to ensure that a complete picture of ransomware attacks in Australia were curated. As acknowledged by the paper, many ransomware attacks result in the sale of data for nefarious purposes, or are driven by other motivations, whether payment is made or not. For this reason, all ransomware attacks should be reported.

Further, it is typically economy and industry-wide matters where information taken from various compromises (i.e Optus, Medibank Private, law firms) are progressively used to attack or exploit higher value services and sectors. Data is not just taken and used from entities and customers pertaining to a single sector. Understanding more of the information and context from all sectors will be useful for organisations to determine the provision of appropriate countermeasures, and the application of targeted and tailored actions that can be taken, and to better understand the broader implications, in the event of a breach of customer data or compromising the wider business operations.

That said, there are existing reporting frameworks for many industries, including the superannuation industry, which is already required to report operational outages for critical systems (including in the case of ransomware) under APRA's prudential standards CPS 230 and CPS 234: Information Security.

The FSC submits that Government should ensure that reporting frameworks are aligned to deliver regulatory efficiencies. This could be achieved if the various Government and regulatory bodies involved communicate with one another and enter into information sharing arrangements for the purposes of adopting a centralised and streamlined approach to reporting and collection data to minimise the regulatory and compliance burden.

Making the reporting process standardised and simplified would also support reducing the reporting burden during a period of crisis where information by an affected business needs to be shared in a manner that is as simple as possible.

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

In its submission to the National Cybersecurity Strategy Consultation in 2023, the FSC called for a streamlined, one stop shop approach to reporting during a cyber incident. A centralised portal would incorporate all industry reporting requirements, allowing relevant agencies and regulators to receive information without the need for an entity to lodge reports separately. The FSC still believes investment in a centralised portal for reporting past and current cyber incidents would greatly assist both directly and indirectly affected parties to report on matters in a streamlined and efficient manner.

Recommendation 1

All organisations should be required to report ransomware attacks in some way, but the reporting regime should reference existing industry regulatory frameworks to minimise the regulatory and administrative impacts on entities.

Question 11: Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?

As noted above, all entities should be required to report ransomware to ensure that the dataset collated from reporting is complete and has utility to drive policy, education and information sharing initiatives. The FSC believes that the threshold question misdirects the problem and narrows the potential benefits of a reporting regime. It is the nature of data and the number of data elements that determine what response is required rather than the turnover of the company that is relevant. This would ensure that companies with low revenues and turnover, but which retain, hold, or manipulate large data sets, are required to report such breaches.

Further, it would ensure that organisations that think they have protected private data by paying the ransom are still reporting the potential loss because it is not always true that paying the ransom prevents the data loss.

The ransomware reporting framework should be aligned to ensure that there is no double reporting obligations for entities that already have regulatory obligations such as superannuation funds through APRA prudential standards.

Question 12: What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?

The FSC submits that expecting organisations to report ransomware incidents in the heat of a cyber-attack is not always tenable. Further, there are existing reporting requirements on varying industries, for example, APRA requires its regulated entities to report incidents within 72 hours.

Given the scope of information to be reported, the FSC submits that the timeframe for reporting should be sufficiently long enough so as not to create additional burden to organisations in a time of crisis.

Recommendation 2

Ransomware reporting timeframes should, where practicable, align with existing reporting requirements but allow sufficient time for entities to manage the crisis of a ransomware attack without adding additional regulatory burden.

Question 13: To what extent would the no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

The FSC is supportive of a no-fault, no-liability approach to reporting of cyber incidents, including ransomware attacks. The no-fault principles will encourage entities to report to the framework which will benefit the community and industry by providing contemporary and accurate data and threat intelligence in relation to ransomware incidents.

Question 15: What is an appropriate enforcement mechanism for a ransomware reporting obligation?

As noted above, reporting obligations should be aligned with existing frameworks to drive regulatory efficiencies. Enforcement action should not be separate from existing mechanisms. Alternatively, where an existing framework is in place, there should be no further enforcement action where any entity has complied with, for example, its APRA obligations but has not yet complied with the new obligation to report. This is in acknowledgement that the provision of another layer of regulation can create or duplicate an additional regulatory and administrative burden on entities, especially those that are closely monitored by independent regulators such as APRA and ASIC.

Recommendation 3

Enforcement frameworks for ransomware reporting should be aligned with existing regulatory enforcement approaches so there is not a double up of regulatory measures.

Question 16: What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, with whom, and in what format?

The FSC is a strong advocate for enabling cross-industry information sharing to assist organisations to uplift their own cyber preparedness. Increased information sharing from government, between industry participants, and even across industries could have a significant impact on an organisation's ability to respond and prepare for threats.

Receiving information in the form of regular briefings and/or secure communications would assist entities to understand the current threat context, including new and emerging threats. In person briefings and cyber threat information sharing sessions also encourage networking among industry peers which further builds on information sharing networks. We note that the National Anti-Scam Centre within the ACCC is also exploring similar issues and channels in the context of intelligence sharing in relation to scams and fraud activity.

Information that would be useful to receive includes:

- ransom amounts requested and/or paid.
- amount and type of data stolen.
- the organisation/individual responsible for the ransomware and other information on the perpetrator, if that can be anonymised.
- Case studies and typologies
- New and emerging threats, and
- Other relevant information on techniques, tactics, and procedures used by the attacker.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Co-ordinator.

Question 17: What should be included in the "prescribed cyber security purposes" for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?

The FSC is supportive of limited use obligations for information shared with the Australian Signals Directorate (**ASD**) and understands the need to balance this with the need to maintain regulatory oversight and enforcement.

The FSC is supportive of the proposed approach outlined in the paper.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board.

Question 21: What limitations should be imposed on the CIRB to ensure that it does not interfere with law enforcement, national security, intelligence, and regulatory activities?

The FSC is supportive of implementing a Cyber Incident Review Board (**CIRB**). The CIRB would help to understand significant cybersecurity events and the learnings would be useful for Australia's business community in uplifting their own cybersecurity preparedness, for example, through the development and publication of education and guidance. That said, the CIRB should have a strict terms of reference that would ensure that it does not create extra red tape for entities as they go through the recovery process after an incident.

Further, the CIRB should have a focus on understanding the event with a lens of learning and uplifting preparedness in the future, as opposed to an enforcement or regulatory function that could potentially double up existing frameworks. For this reason, the FSC is supportive of the no-fault principle outlined in the paper.

Recommendation 4

The Cyber Incident Review Board should have a terms of reference that focusses on understanding a cyber incident with a view to uplifting preparedness in the future, as opposed to an enforcement or regulatory function.

Question 23: What factors would make a cyber incident worth reviewing by a CIRB?

There should be, where practicable, a clear and transparent framework for determining what factors the CIRB may consider review following a cyber incident, while clarifying those matters which fall outside of any review process. This framework should be public. Factors the FSC believes are relevant to whether the CIRB reviews an event or not include:

- The size of the organisation involved.
- If the event affected multiple organisations
- The number of customers or stakeholders affected by the event.
- The nature, content and severity of the data that has been affected (if applicable)
- The severity of the outage caused by the incident (if applicable) and the impact and extent of disruption to operations.
- Details of any communications with or from the source/s of the cyber attack
- The methods employed in the cyber-attack.
- The response to the event by the relevant organisation and the actual or expected or actual recovery time.

Further, as the National Cybersecurity Coordinator currently has the power to lead coordination responses on 'major cyber incidents' there should be significant overlap in how the Coordinator determines if something is a 'major cyber incident' and what gets referred to the CIRB.

It is reasonable that the CIRB would maintain a right to investigate any event it saw fit however, this should be carefully constructed in conjunction with the charter dictating who would be a member of the CIRB to ensure that there were no conflicts of interest in relation to this power.

Recommendation 5

The Cyber Incident Review Board should have a clear, transparent and published framework to consider when determining whether to investigate a cyber incident.

Question 24: Who should be a member of a CIRB? How should these members be appointed?

The CIRB should be made up of members that have both cybersecurity and technology expertise as well as relevant industry knowledge. For example, were an event to occur within the superannuation industry, some CIRB members should have superannuation and/or financial services knowledge to provide the necessary insights and understanding of the impacts. It would not be productive for the CIRB to continually have to be schooled on a particular industry's operating context during each review. Acknowledging it is not possible to have representatives from every industry, these industry experts could be from areas where cybercrime is more likely such as various financial service industries and the telecommunications industry. It may also be useful, where appropriate, to consider a chair from a regulatory body such as APRA.

Further, there should be mechanisms in place to ensure that CIRB members remain impartial. For this reason, the CIRB might benefit from an experienced, independent chair with a strong work history encompassing fields such as governance and law.

Recommendation 6

The Cyber Incident Review Board should have members with a strong understanding of cybersecurity and technology as well as rotating members who have industry specific knowledge and expertise for key industries likely to be targeted by cybercrime.

Question 28: Who should be responsible for initiating reviews to be undertaken by a CIRB?

As noted above, there should be a robust and transparent framework for whether a cyber incident should be referred to the CIRB or not. This would mean the power to initiate an investigation would sit with the CIRB. The CIRB could also retain power to investigate matters outside of the framework, where it can make an impartial case to do so.

The FSC is supportive of the Minister also maintaining legislated powers to refer a matter to the CIRB however, the considerations for the Minister to refer a matter to the CIRB, however, such a power should be prescribed in appropriate legislation and/or regulation and should include a similar need to make a case with respect to the existing framework.

Wherever the power to refer matters to CIRB rest, there should be clear, transparent and public frameworks for what matters will be referred to ensure entities are put on appropriate notice about the process for CIRB reviews.

Recommendation 7

Whatever body or person is responsible for referring matters to the Cyber Incident Review Board, the decision-making framework should be clear, transparent and published.

Question 29: What powers should a CIRB be given to effectively perform its functions?

In order for the CIRB to be effective, It will require wide ranging investigative supported by appropriate information gathering powers. This, however, should be balanced with existing regulatory frameworks (e.g., privacy) and matters such as legal and professional privilege.

The powers should also seek to align and acknowledge that many industries have existing regulatory interventions in the wake of a significant impact and organisations may be dealing with multiple notices from the likes of APRA, ASIC, ATO, law enforcement (e.g., AFP), and AUSTRAC. Whatever investigative powers the body is given, they should be narrow and specific so as not to put undue burden on organisations having to expend significant resources responding to a CIRB enquiry. The FSC submits that Government should conduct further consultation once a model is proposed to ensure that industry can provide input based on more specific detail.

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers.

Question 37: How would a directions power assist you in taking action to address the consequences of an incident?

The FSC is supportive of a directions power which allows for better communication during and in the immediate aftermath of an event. As noted in the paper, the Government could not share details about affected persons with banks. The superannuation industry would have also benefited from access to information about personal data that had been stolen to better protect their customers from potential fraud.

Incidents often affect more than one entity and more than one industry. Having a directions power, and a solid framework of understanding about how that directions power will be deployed will be key to ensuring that it is used effectively. For example, understanding how interested parties can gain access (or apply to gain access) to relevant information about stolen identity information as soon as practicable.

Question 38: What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?

As previously mentioned, some FSC members, specifically superannuation funds, are subject to APRA prudential rules. This includes CPS 230 which provides APRA sweeping powers to provide directions in relation to operational risk preparedness including risk profile and business continuity planning. Government should ensure that any directions power is not inconsistent with the approaches outlined in these prudential standards.

Another legislative framework to be aware of are the AUSTRAC 'tipping off' prohibitions at section 123 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, which prevent organisations from discussing sharing information where it involves the submission of suspicious

matter reports (**SMRs**). These reports are submitted by organisations to AUSTRAC combat money laundering and terrorism financing and other serious economic crimes. The tipping off provisions mean that organisations essentially cannot discuss the submission of these SMRs for fear that it may alert the subject of the report to the potential investigation by law enforcement. These provisions currently stifle the ability of organisations to share meaningful and intelligence information about cybersecurity incidents and may also contradict any effort by government to later share information in the way described in the consultation paper.

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions.

Question 41: How would a move towards a 'harm-based' threshold for information disclosure impact your decision-making? Would this change make it easier or more difficult to determine if information held by your asset should be disclosed?

The FSC is supportive of measures that increase the ability of government and industry to share information about current cyber incidents and threats. Therefore the FSC is supportive of a 'harm-based' approach to considering whether information should be shared.

The FSC believes that in addition to a harm-based paradigm, this should be balanced with the benefits that will be incurred with the free sharing on contemporary and contextual information during and after an event.

The Government should also be clear about the use of the information and as far as practicable, be transparent about how the information will be disseminated. This will allow for organisations to better understand how the data they are sharing will be used and give them confidence in the sharing of that information.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers.

Question 42: How would the proposed review and remedy power impact your approach to preventative risk?

As noted previously, APRA regulated entities are subject to CPS 230, a prudential standard focussed on operational resilience. Under this standard, APRA have broad powers to review business continuity plans and require amendments where it feels a regulated entity needs to improve.

Currently, much of superannuation funds obligations under the critical infrastructure regime are deferred to APRA so that compliance with prudential standards, means compliance with SOCI requirements. The FSC believes that this framework works well and avoids a duplication of regulatory interventions.

The FSC submits that Government should carefully consider how the proposed remedy power interacts with the existing framework to ensure that APRA regulated entities do not end up in a situation where there are many parties making required changes to internal operating plans or that requested changes are inconsistent with each other.

Recommendation 8

Government should defer its remedy and review power to an appropriate regulator, such as APRA, where appropriate.

The paper proposes to give the Secretary of Home Affairs the review and remedy power where there is a serious deficiency. Notwithstanding the above recommendation, the FSC submits that what constitutes a serious deficiency should be further unpacked and clarified to provide certainty to industry.

If you have any questions about this submission, please do not hesitate to get in touch.

Yours sincerely,

Kirsten Samuels
Policy Director, Superannuation and Innovation

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