SUBMISSION

Submission to the Department of Home Affairs — 2023–2030 Australian Cyber Security Strategy: Legislative Reforms: Consultation Paper

29 February 2024

The Association of Superannuation Funds of Australia Limited
Level 11, 77 Castlereagh Street
Sydney NSW 2000

PO Box 1485
Sydney NSW 2001

T +61 2 9264 9300
1800 812 798 (outside Sydney)
F 1300 926 484
W www.superannuation.asn.au

ABN 29 002 786 290 CAN 002 786 290

File: 2024/10

Department of Home Affairs
101 George Street
Parramatta NSW 2150

Lodged via consultation web form: Cyber Security Legislative Reforms: consultation on proposed new cyber security legislation and on changes to the Security of Critical Infrastructure Act 2018 (homeaffairs.gov.au)

29 February 2024

Dear Sir/Madam,

Consultation on proposed new cyber security legislation and on changes to the Security of Critical Infrastructure Act 2018

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission in response to your consultation on proposed new cyber security legislation and on changes to the Security of Critical Infrastructure Act 2018.

ABOUT ASFA

ASFA, the voice of super, has been operating since 1962 and is the peak policy, research and advocacy body for Australia's superannuation industry. ASFA represents the APRA regulated superannuation industry with over 100 organisations as members from corporate, industry, retail and public sector funds, and service providers.

We develop policy positions through collaboration with our diverse membership base and use our deep technical expertise and research capabilities to assist in advancing outcomes for Australians.

GENERAL COMMENTS

ASFA is broadly supportive of the new cyber security legislation and proposed amendments to the *Security of Critical Infrastructure Act 2018* (SOCI Act), to improve cyber security and the security of critical infrastructure.

SPECIFIC COMMENTS

In reviewing the Consultation Paper, our member organisations have made the following observations and recommendations**.**

1. Part 1: New cyber security legislation

Measure 1 - Limited Use Obligation

Member organisations have indicated that this approach may not be sufficient to overcome industry hesitancy to engage with the Australian Signals Directorate (ASD) / Department of Home Affairs (DHA) with respect to cyber events, or minimise the likelihood of organisations directing the ASD through their legal department as opposed to their incident response teams.

In addition, third party administrators may be more likely to be caught by more aspects of the SOCI Act than are superannuation funds trustees, (for example Risk Management Plans, reporting owner/operator information to the CISC).

Member organisations have provided the following considerations:

1. for the purposes of Professional Indemnity (PI) insurance, and given the multitude of legal and contractual obligations to navigate, as a matter of course cyber events routinely will be sent to the legal department for consideration
2. the Assistance and Intervention powers available to the Minister under the SOCI Act, especially section 35AC[1] in directing the ASD are extensive. We acknowledge that these are intended to be used as a last resort, but prima face they appear to be excessive
3. with respect to an administrator, any ASD involvement or actions would need to go through an organisations legal department first, to ensure that any ASD actions do not result in the administrator breaching any contractual obligations to their superannuation fund clients, which in turn relate to legislative obligations or prudential standards imposed on trustees
4. service providers are likely to require engagement with the superannuation fund trustee before approaching the Australian Cyber Security Centre (ACSC) / Cyber and Infrastructure Security Centre (CISC) - thus involving the trustee's lawyers in addition to the administrator and any PI lawyers.

Whilst our member organisations appreciate the Government's aims to help manage events and the wider economic impacts, they are concerned that, from a superannuation perspective, the SOCI Act potentially is too blunt an instrument, and that the proposals do not give sufficient weight to existing regulatory and contractual obligations.

Measure 2: Further understanding cyber incidents - Ransomware reporting for businesses

ASFA supports the reporting of ransomware incidents.

Our member organisations appreciate the benefits of threat intelligence sharing across the superannuation sector, however, they believe that more needs to be done to ensure the anonymity of reporting entities. There are likely to be occasions where it is critical to ensure anonymity, in particular as we believe that this, in itself, would greatly encourage businesses to self-report.

In addition, our members consider it important to take into consideration current reporting requirements when creating additional reporting obligations.

ASFA strongly encourages policy makers to work with the regulators to devise a way to streamline cyber incident reporting.

Legislation Measure 3 - Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

To increase engagement with the Australian Signals Directorate (ASD) in the superannuation sector, member organisations have observed that it would be helpful if the terminology used, and the regulatory obligations imposed under the Australian Prudential Regulatory Authority (APRA)'s Cross-Industry Prudential Standard 234 (CPS 234)[2] were to be aligned.

This would make any notification to the ASD notifiable to APRA, as clarified by CPS 234[3], which extends the obligation to report to APRA to incidents reported to domestic government agencies, such as the ASD.

[1] Part 3A
[2] Paragraph 35(b)
[3] Footnote 14

The threshold for security incident reporting to APRA under CPS 234, however, is set at information security incidents "that materially affected, or had the potential to materially affect, financially or non-financially, the entity…".[4] Member organisations have observed that it may be considered that engagement with ASD during minor incidents does not meet this materiality criteria.

While the 'Safe harbour' consideration is valid, it will be important to clarify the extent of incident reporting obligations, to both international and Australian regulators, as a result of engagement with the ASD.

ASFA recommends that consideration be given to

1. policy makers working with the regulators to devise a way to streamline reporting
2. either:
    - making clarifications in the legislation to the effect that:
        - the ASD is not a regulatory body
        - reporting security incidents or events to the ASD does not automatically create an obligation under APRA CPS 234[5] to report to APRA; or
    - creating a provision for security management support services for entities responding to security events, as opposed to incidents. This would create a clear separation between regulated incident reporting under the SOCI Act and the proposed Ransomware Reporting regime, and other security events/low impact incidents, which would support ASD's statutory function to provide cyber security advice and assistance to industry and the community.

Recommendations

1. That policy makers working with the regulators to devise a way to streamline reporting
2. That either:
    - clarification should be made in the legislation to the effect that:
        - the ASD is not a regulatory body
        - reporting security incidents or events to the ASD does not automatically create an obligation under APRA CPS 234[6] to report to APRA; or
    - a provision should be created for security management support services for entities responding to security **events**, as opposed to incidents.

2. Part 2: Amendments to the Security of Critical Infrastructure Act 2018

Measure 5 - Protecting critical infrastructure – Data storage systems and business critical data

2.1. Scope of Critical Data Storage and Processing Asset sectors should be more clearly defined

Our members organisations have indicated that greater clarity around obligations is welcome.

The Security Legislation Amendment (Critical Infrastructure) Act 2021 (Act) defines the concept of Business Critical Data in a broad terms. The Act applies the definition under section 12F, used exclusively with respect to a Critical Data Storage or Processing Asset, to superannuation as one of the regulated industry sectors, however, this definition is problematic.

[4] Paragraph 35(a)
[5] Paragraph 35 (b)
[6] Paragraph 35 (b)

Our member organisations have noted that the proposals is to expand definitions to capture data storage systems but they do not include clarifying the definition of Data Storage or Processing.

At issue is the lack of clarity around the definition under section 12F – the CISC has provided its views on the definition, noting that it is new and it has not been tested by the courts. The CISC has indicated that where data storage or processing is a primary or secondary service offering, the entity would be caught under the Act, but where data is ancillary (e.g. accounting services), the entity would not be caught.

This distinction, while significant to the entities potentially affected by the obligations, matter little to a person whose personal details have been exposed in a cyber event. It is suggested that the definition of 'used wholly or primarily to provide a data storage or processing service' be amended either to clarify the distinction, or else to remove it.

In the superannuation sector there are indications that potentially only hyper-cloud providers accept they have obligations under the SOCI Act as Critical Data Storage or Processing Asset operators.

Our member organisations have indicated that there is a tendency for other cloud and business-process outsourcing suppliers – which in superannuation includes Fund Administrators, Custodians, Payroll Providers, Marketing Technology Providers, Security Technology Suppliers – to consider they are not operators of a Critical Data Storage or Processing Asset. This does not always take into account the risks to critical superannuation asset created by cloud and business process outsourcing providers.

In the superannuation sector this risk is elevated due to its reliance on personal information for customer identification (for example Date-of-Birth), in accordance with the ATO's SuperStream framework, and the absence of industry specific identifiers, such as BSB/Account Number and PayID that are used in the banking sector. Often in data breaches in other sectors it is this general, personal, information that is leaked, which serves to increase risks to the superannuation sector.

2.2. Extending necessitates adjustment for sector specific threats, circumstances & regulation

Our member organisations have observed that extending this to all sectors, without adjusting for the specific threats, circumstances, and regulatory obligations of each sector, would create additional unnecessary compliance burdens as follows.

2.3. Definition of Business-Critical Data

The definition of Business-Critical Data in the Act includes 'information related to research & development of a critical infrastructure asset'.

Our member organisations have observed that, in the superannuation sector, this means that benign demographic and aggregated information, such as that used for data modelling for retirement product development, could be considered business critical and essential for the operation of the critical superannuation asset. They have indicated that the obligations would place additional restrictions on the use of that data that would negatively affect the superannuation sectors' implementation of their obligations under the retirement income covenant imposed under the *Superannuation Industry (Supervision) Act 1993*.

2.4. Need to avoid the duplication of regulatory obligations

Our member organisations have recommended that specific consideration should be given to each sector to avoid duplication of regulatory obligations.

In the superannuation sector there is APRA's Operational Risk Management Prudential Standard CPS 230, which covers similar matters with respect to operational resilience, that comes into effect from 1 July 2025.

In addition, member organisations have welcome the contemplation of the upcoming Privacy Act changes and recommend that the Consumer Data Right (CDR) also be considered and that analysis be performed to identify any further legislation that could touch on the proposed measures.

Recommendations

3. That specific consideration should be given to each sector to avoid duplication of regulatory obligations, including contemplation of the upcoming Privacy Act changes.
4. That the Consumer Data Right (CDR) also be considered.
5. That analysis be performed to identify any further legislation that could touch on the proposed measures.

Before specific obligations are applied broadly under the SOCI Act, the upcoming reforms to the Privacy Act should be considered. If applied to all SOCI Act sectors, without further sector-specific consultation to identify and clarify obligations and requirements, and assessment of those obligations, the breadth of the personal information definition could serve to expand significantly the scope and number of critical assets, creating additional complexity with respect to managing privacy incidents in complicated supply chains.

Member organisations have noted that:

- the Privacy Act essentially is a framework for managing privacy and securing data, with some ability for individuals to have control over their data
- the CDR essentially is a data portability framework (giving individuals control over their data), which then has obligations with respect to managing privacy and security overlayed on top.

We note it could take some time and effort to align measures that are designed to achieve differing legislative intents.

Member organisations have noted that, in practice, third party service providers effectively already are caught by the SOCI Act and the prudential standards that apply to their customers (SPS 220/CPS 230, CPS 234, CPG 235.

When it comes to the superannuation sector our member organisations made the following recommendation and observation:

- increased regulatory reporting requirements need to take into consideration the likelihood of multi-party breaches. A recent anecdote illustrating this phenomenon is that Optus had to report to the Office of the Australian Information Commissioner (OAIC) that the OAIC reported to Optus that HWL Ebsworth (HWLE) reported to the OAIC that there was some Optus data in the OAIC data in the HWLE breach that was notifiable to the OAIC.
- while the data leaked in those breaches had impacts on critical superannuation assets, none of these actors were subject to the SOCI Act, which serves to indicate that the SOCI Act may not be the optimal instrument to introduce these business-critical data obligations. The SOCI Act was introduced to increase resilience, continuity of operations and reduce foreign interference risks - extending it to drive increased protection of personal data adds unnecessary complexity and results in the duplication of regulatory obligations.

Recommendation

6. That regulatory reporting requirements need to take into consideration the likelihood of multi-party breaches.

2.5. Need to consider when sector does not operate on a real-time basis

Member organisations have observed that directly extending obligations to the superannuation sector does not take into consideration that substantial operations in the sector do not operate on a real-time basis, instead completing batch-processing with the ATO, gateway operators and clearing houses.

In addition, these sector participants are not direct suppliers to superannuation funds, which makes it impractical to apply contract based SOCI Act responsibilities and obligations. This ecosystem already is regulated by the ATO, APRA, ASIC, and the Gateway Network Governance Body (GNGB), which are better placed to address security challenges within this regulated ecosystem.

2.6. Amendments should clarify sector-specific obligations and thresholds

Our member organisations have indicated that the amendments should clarify sector-specific obligations and thresholds for incidents with significant and relevant impacts for each sector.

For superannuation, it will be important to clarify whether the significant impacts are confined to the investment operations of the superannuation fund, given that the application of the SOCI Act to superannuation was based on Funds Under Management (FUM) and not the total number of customers.

2.7. Need to explain how regulated critical asset operators benefit from increased reporting

Our member organisations have observed that where there is a disclosed relevant incident impacting large volumes of personal information, the Consultation Paper does not explain how regulated critical asset operators benefit from increased reporting to accelerate a response.

For large-scale identity information breaches in the financial services and superannuation sectors, visibility and understanding of the critical asset operator ecosystem and intelligence sharing is essential. This would support the objectives of the *2023-2030 Australian Cyber Security Strategy Shield 3: World-class threat sharing and blocking*.

2.8. Consultation Paper recognises sufficient regulation in super sector by other frameworks

Our member organisations have observed that the Consultation Paper correctly recognises that there is sufficient regulation in the superannuation sector through other frameworks, such as APRA's CPS 234.

We commend the decision by the Minister, on the basis that existing APRA prudential standards include comparable obligations, not to activate specific obligations, such as asset register reporting, with respect to superannuation.

Given this, ASFA recommends that consideration be given to:

1. revising the Business-Critical Data definition such that it:
    - defines a clear condition that is based on the simultaneous satisfaction of multiple criteria, where the potential impact on the critical asset is considered in combination with the 20,000 individuals volume threshold for personal information. The condition should contain a provision for compensating controls, such as data encryption, to be used to reduce the sensitivity of the dataset and remove the business-critical data designation
    - takes into account the nature of each sector, and excludes criteria that is not applicable. By way of example, in the superannuation sector, Research & Development (R&D) or risk information, with extensive reporting and public disclosure obligations, has a significantly different risk/threat profile than similar information with respect to a water utility.

2. avoiding creating separate breach-reporting obligations for privacy breaches. Instead, we submit that consideration should be given to utilsing centralised privacy breach reporting through the existing OAIC reporting mechanism, with the OAIC forwarding large-scale breach notifications to the CISC/ASD. This modification would also serve to address the issue of cloud operators handling large volumes of personal information but, if they are not directly subject to the SOCI Act, they are not obliged to report relevant breaches to the CISC/ASD.
3. clarifying the scope of the existing Critical Data Storage or Processing Asset obligations to apply directly to all data processors handling sensitive personal or identity information of more than 20,000 individuals, including cloud software and payroll providers.
4. publishing sector-specific definitions and clarification with respect to the scope and thresholds for significant and relevant incidents, taking into account the unique characteristics of each sector. By way of example, in the superannuation sector, there should be clarification as to whether significant impact incidents apply only to the custodian with respect to the fund's investment operations. The CISC has published guidance with respect to specific attacks (e.g. telephone 'denial of service' is not reportable) but has not extended this guidance to each sector.
5. requiring the disclosure of critical asset operators to other participating organisations in the regulated SOCI Act ecosystem, to simplify the management of supplier obligations under the SOCI Act, assist consistency and mitigate the likelihood of self-selection and the avoidance of compliance obligations. This would reduce the compliance burden of adding SOCI Act obligations to contracts with overseas suppliers.

Recommendations

7. That the Business-Critical Data definition be revised such that it:
    - defines a clear condition that is based on the simultaneous satisfaction of multiple criteria, where the potential impact on the critical asset is considered in combination with the 20,000 individuals volume threshold for personal information
    - takes into account the nature of each sector, and excludes criteria that is not applicable
8. That creating separate breach-reporting obligations for privacy breaches be avoided.
9. That the scope of the existing Critical Data Storage or Processing Asset obligations be clarified to apply directly to all data processors handling sensitive personal or identity information of more than 20,000 individuals, including cloud software and payroll providers.
10. That sector-specific definitions and clarification regarding the scope and thresholds for significant and relevant incidents be published, taking into account the unique characteristics of each sector.
11. That disclosure of critical asset operators to other participating organisations in the regulated SOCI Act ecosystem be mandated.

Measure 8: Enforcing critical infrastructure risk management plans (CRIMP) – review and remedy powers

While greater oversight is useful, it should be noted that the CIRMP elements of the SOCI Act are focused on risk processes and that this measure is focused primarily on the absence of a legislative framework that allows the regulator to issue a direction to an entity to remedy a deficient risk management program.

While SPS 220 is framed similarly, APRA has indicated that CPS 230 shifts the emphasis to focus on risk outcomes. We recommend that consideration be given to amending the language of the CIRMP obligations to focus on outcomes for customers, as opposed to devising, and adhering to, internal risk processes.

Our member organisations believe that more should be done to encourage entities to submit their CIRMP programs/plans for a consequence free, no cost, evaluation.

Further, we recommend resourcing regulators to assist entities to proactively protect their assets, which would make it easier to identify areas for improvement.

Recommendations

12. That consideration be given to amending the language of the CIRMP obligations to focus on outcomes for customers, as opposed to devising, and adhering to, internal risk processes.
13. That more should be done to encourage entities to submit their CIRMP programs/plans for a consequence free, no cost, evaluation.
14. That regulators are resourced to assist entities to proactively protect their assets, which would make it easier to identify areas for improvement.

****

If you have any queries or comments in relation to the content of our submission, please contact Fiona Galbraith, Director Policy, on 0431 490 240 or by email fgalbraith@superannuation.asn.au.

Yours sincerely

Mary Delahunty
Chief Executive Officer