



SUBMISSION

Parliamentary Joint Committee on Intelligence and Security – Cyber Security Legislative Package 2024

25 October 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: 2024/42

Senator Raff Ciccone
Chair of the Parliamentary Joint Committee on Intelligence and Security
Parliament House
Canberra ACT 2600
Via email: pjcis@aph.gov.au
11 October 2024

Dear Senator Ciccone,

Parliamentary Joint Committee on Intelligence and Security – Inquiry into the Cyber Security Legislative Package 2024

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission in response to this consultation by the Parliamentary Joint Committee on Intelligence and Security (the Committee).

About ASFA

ASFA 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.

ASFA has a keen focus on matters that impact the outcomes achieved by individuals through the superannuation system, their experiences with the system, and issues that impede the industry's operational effectiveness.

ASFA's Opening Comments

ASFA broadly supports this legislative package, noting that it is composed of three pieces of legislation:

1. the Cyber Security Bill 2024 ([the Cyber Security Bill](#))
2. the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 ([the SOCI Amendment Bill](#)), and
3. the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024 ([the Intelligence Services Bill](#)).

When this package was released on 9 October 2024, by the Minister for Home Affairs and Cyber Security, the Hon. Tony Burke MP (the Minister) made the following statement, with which ASFA strongly agrees:¹

Australia currently faces heightened geopolitical and cyber threats, which means that our critical infrastructure is increasingly at risk. The risk to our sovereignty, defence, and security has never been more present, especially for the critical infrastructure providing essential services crucial to our way of life.

¹ *Commonwealth Parliamentary Debates*, House of Representatives, [9 October 2024](#), 48 (The Hon. Tony Burke MP) (Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 – Second Reading Speech).

The Minister went on to say that the purpose of these reforms is to:²

[B]uild upon previous reforms [and] enhance the security, resilience and agility of critical infrastructure in the face of an increasingly hostile and complex threat and risk landscape.

ASFA supports reforms targeted at dealing with these key issues of cyber security in a rising threat environment. We note these reforms follow a long process of consultation on how best to improve the relevant policy settings, which included:

1. the release of Australia's National Cyber Security Strategy 2023-2030 on [22 November 2023](#)
2. the creation of the Executive Cyber Council on [22 November 2023](#), to facilitate co-leadership between government and industry on cyber issues.
3. the appointment of the National Cyber Security Coordinator, Lieutenant General Michelle McGuinness CSC, from [26 January 2024](#)
4. the Department of Home Affairs' (DHA) consultation on the Cyber Security Legislative Reforms Consultation Paper, closing on [1 March 2024](#)

ASFA made a submission to the Cyber Security Legislative Reforms Consultation Paper on [29 February 2024](#), which is **Attachment C** of this submission. There, we said:³

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.

Notwithstanding our broad support for the reforms, we made recommendations on the following aspects of the changes to ensure that the underlying intent was actualised in a way that would be most effective. These recommendations related to the following topics.

1. the limited use obligation proposed to be created in the SOCI Act and Intelligence Services Act⁴
2. the reporting of ransomware incidents⁵
3. measures designed to increase engagement with the National Cyber Security Coordinator (NCSC) and Australian Signals Directorate (ASD) during cyber incidents⁶
4. amendments to the SOCI Act regarding data storage systems and business critical data⁷
5. additional powers for the Government to review and remedy serious deficiencies in Critical Infrastructure Risk Management Plans.⁸

Consistent with ASFA's earlier submission on this issue, while supporting the reform of Australia's cyber security laws, this submission will observe where the proposals could be adjusted to better achieve their underlying

² *Commonwealth Parliamentary Debates*, House of Representatives, [9 October 2024](#), 48 (The Hon. Tony Burke MP) (Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 – Second Reading Speech).

³ ASFA, Submission to Home Affairs on the Cybersecurity Legislative Reforms Consultation Paper ([29 February 2024](#)), 2.

⁴ *Ibid*, 2-3. This is dealt with in Part 4 of the Cyber Security Bill in this package and Schedule 1 of the Intelligence Services Bill.

⁵ *Ibid*, 3. This is dealt with in Part 3 of the Cyber Security Bill in this package.

⁶ *Ibid*, 3-4. This is dealt with in Part 4 of the Cyber Security Bill in this package and Schedule 1 of the Intelligence Services Bill.

⁷ *Ibid*, 4-8. This is dealt with in Schedule 1 of the SOCI Amendment Bill in this package.

⁸ *Ibid*, 8-9. This is dealt with in Schedule 4 of the SOCI Amendment Bill. See too

goals. The feedback from our earlier submission to DHA on these matters continues to reflect the ASFA's position. Which is why we have attached that earlier submission for consideration in **Attachment C**.⁹

In addition to our previous submission on the cyber security reforms, ASFA would also like to draw the Committee's attention to some further initiatives which our members have proactively committed to, as a sign of ASFA's desire to work collaboratively with the Government to strengthen protections in the cybersecurity space and combat financial crime. These are the following:

1. ASFA's Better Practice Guidance on Minimum Fraud Controls for Superannuation Funds ([here](#))
2. ASFA's Financial Crime Protection Initiative ([FPCI](#)), which seeks to help industry and consumers work together to fight financial crime through:
 - Enhancing collaboration and knowledge sharing between funds and critical service providers including custodians, administrators and tech providers
 - Developing industry-wide frameworks to combat financial and cybercrime
 - Connecting the superannuation sector, relevant government agencies and related financial services bodies
 - Helping make Australians aware of the actions they can take to protect their super and data from scammers.
3. ASFA's [recent submission](#) on reforming Australia's Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) regime.
4. ASFA's [4 October 2024](#) submission on the Scams Prevention Framework draft legislation, where we said:¹⁰

ASFA wishes to emphasise that our \$3.9 trillion sector wants to assist the Government in dealing with scams. Our membership has been on the front foot in proactively seeking combat scams and issues related to other heinous forms of financial crime.

5. ASFA's [11 October 2024](#) submission on the reforms to Australia's privacy laws, where we agreed with the Attorney-General, the Hon Mark Dreyfus KC MP, that:¹¹

Strong privacy laws and protections are critical to building public trust and confidence in the digital economy, and driving the investments needed to keep people's data safe. The right to privacy is a fundamental human right.

6. ASFA's [recent appearance](#) before the Parliamentary Joint Committee on Corporations and Financial Services inquiry into the Financial Services Regulatory Framework in Relation to Financial Abuse and [joint statement](#) on this topic with the Super Members Council and Women in Super. There, we called for – 'urgent legal reform to stop abusers getting victim's super.'

The above summary of our recent work around financial crime, AML/CTF, scams, privacy and financial abuse demonstrates ASFA's commitment to strong cyber security laws is part of a wide range of activities we are undertaking to combat all forms financial crime. These various types of financial crime, including cyber incidents, need to be viewed holistically and as interrelated, as do any regulations which seek to combat them.

⁹ ASFA, Submission to Home Affairs on the Cybersecurity Legislative Reforms Consultation Paper, 2 ([29 February 2024](#))

¹⁰ ASFA, Submission to Treasury on the Scams Prevention Framework – Exposure Draft Legislation ([4 October 2024](#)).

¹¹ *Commonwealth Parliamentary Debates*, House of Representatives, [12 September 2024](#), 21 (The Hon. Mark Dreyfus KC MP)(Privacy and Other Legislation Amendment Bill 2024 – Second Reading Speech)

Given the volume of reforms proposed in this package, ASFA intends to focus our comments on those areas which are most relevant to the superannuation sector. These are as follows:

In the Cyber Security Bill:

1. the mandatory ransomware payment reporting obligations (Part 3)
2. the limited use obligation with the NCSC (Part 4)
3. the creation and role of the Cyber Incident Review Board (Part 5)
4. the security standards for smart devices (Part 2).

In the SOCI Amendment Bill:

5. the requirement for data storage systems holding business critical data to be regulated as critical infrastructure assets (Schedule 1)
6. the new government consequence management powers, including the power to direct an entity to take action to respond to 'incidents', not just 'cyber incidents' (Schedule 2)
7. the new definition of 'protected information', which includes a harms-based assessment and a non-exhaustive list of relevant factors clarifying when information can be shared or used for other purposes (Schedule 3)
8. the new power for the regulator to issue directions to responsible entities to address any 'serious deficiencies' in their Critical Infrastructure Risk Management Programs (CIRMP) (Schedule 4).

In the Intelligence Services Bill:

9. the new limited use obligation protecting information voluntarily given to the Australian Signals Directorate (ASD) during an impacted entity's engagement on a cyber incident. This complements Part 4 of the Cyber Security Bill.

Attachment A of this submission will first outline what is proposed by each of these reforms. It will then make ASFA's recommendations regarding each proposal.

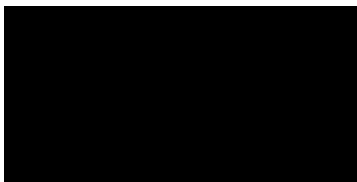
Attachment B provides a useful summary of the package.

Attachment C includes a copy of ASFA's 29 February 2024 submission to DHA on this package.

We would welcome the opportunity to elaborate on our recommendations with you further.

Please feel free to reach out to ASFA Senior Policy Advisor, [REDACTED], at [REDACTED], should you have any questions or wish to discuss these matters in detail.

Yours sincerely



James Koval

Head of Policy and Advocacy

Table of Contents

ASFA’s Opening Comments	1
Attachment A – ASFA’s Detailed Views on Specific Proposals	6
A. The Cyber Security Bill	6
1.1 the mandatory ransomware payment reporting obligations	6
1.2 ASFA’s recommendations	7
2.1 The limited use obligation with the National Cyber Security Coordinator (NCSC)	7
2.2 ASFA recommendations	8
3.1 The creation and role of the Cyber Incident Review Board	9
3.2 ASFA’s recommendations	10
4.1 The security standards for smart devices	10
4.2 ASFA’s recommendations	10
B. The SOCI Amendment Bill	11
5.1 The requirement for data storage systems holding business critical data to be regulated as critical infrastructure assets	11
5.2 ASFA’s recommendations	11
6.1 The new government consequence management powers, including the power to direct an entity to take action to respond to incidents, not just cyber incidents	12
6.2 ASFA’s recommendations	13
7.1 The new definition of ‘protected information’, which includes a harms-based assessment and a non-exhaustive list of relevant factors clarifying when information can be shared or used for other purposes	13
7.2 ASFA’s recommendations	13
8.1 The new power for the regulator to issue directions to responsible entities to address any serious deficiencies identified in Critical Infrastructure Risk Management Programs (CIRMP)	14
8.2 ASFA’s recommendations	14
C. The Intelligence Services Bill	15
9.1 The new limited use obligation protecting information voluntarily given to the ASD during an impacted entity’s engagement on a cyber incident to complement Part 4 of the Cyber Security Bill.	15
9.2 ASFA’s recommendations	15
Attachment B – ASFA’s Summary of the Proposals	
Attachment C – ASFA’s Past Submission on the Package (29 February 2024)	Error! Bookmark not defined.

Attachment A – ASFA’s Detailed Views on Specific Proposals

A. The Cyber Security Bill

1.1 the mandatory ransomware payment reporting obligations

The mandatory ransomware payment reporting obligations are contained within Part 3 of the Cyber Security Bill. They are summarised in the simplified outline in clause 25.

ASFA notes this proposal implements Measure 2 from the DHA’s Legislative Reforms Consultation Paper.¹²

The Explanatory Memorandum outlines that:¹³

This Part establishes a reporting obligation which is imposed on certain entities who are impacted by a cyber security incident, and who have provided or are aware that another entity has provided, a payment or benefit (which is referred to as a ransomware payment) to an entity that is seeking to benefit from the impact or the cyber security incident.

In understanding this Part, regulated entities will need to have regard to the following:

- Clause 26 establishes when ransomware reporting obligations are enlivened. These include:
 - if a cyber incident is ‘occurring or imminent’ and it could ‘reasonably be expected to have a direct impact’ on the regulated entity.¹⁴
 - the entity must be aware of a ‘demand’ made by the ‘extorting entity’ that would cause them to ‘benefit’ from the incident.¹⁵
 - the obligation to report is enlivened if the regulated entity provides a payment to the extorting entity, either directly or through a third party, which is directly related to the demand.¹⁶
 - the entity must meet the ‘turnover threshold’ prescribed in regulations under clause 26(3).
- Clause 27 outlines what an entity must do when their reporting obligations are enlivened under this Part, this includes:
 - providing the ‘designated Commonwealth body’ with a copy of the ransomware payment report within 72 hours of being made aware a payment has been made.¹⁷
 - the report should contain – the regulated entity’s contact and business details, the nature of the cyber security incident (including its impact on the regulated entity), the demand made by the extorting entity, details of the ransomware payment (in the form approved by the Secretary and as prescribed by the rules) and communications with the extorting entity in relation to the incident, the demand and the payment.

¹² 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper ([December 2023](#)), 16.

¹³ Explanatory Memorandum, Cyber Security Bill 2024 ([Cth](#)) 39[178].

¹⁴ Clause 26(1)(a)-(c). Please note, the term ‘cyber incident’ is defined in clause 10 and this should be read alongside the presumption in clause 26(4).

¹⁵ Clause 26(1)(d).

¹⁶ Clause 26(1)(e).

¹⁷ Clause 27(1). Note that the designated Commonwealth body will be prescribed in the Rules or will otherwise be the ASD, pursuant to clause 8.

- Clause 28 excludes a reporting entity from actions or proceedings for damages in relation to an act done of omitted, 'in good faith', in compliance with section 27.¹⁸

Regulated entities that fail to report ransomware payments in accordance with this Part could lead to civil penalties of \$18,780.¹⁹

1.2 ASFA's recommendations

In relation to Part 3 of the Cyber Security Bill, ASFA has the following recommendations:

- On clause 26 - we seek from detailed guidance and examples on certain terms in the legislation which are open to interpretation, including when a cyber incident could properly be said to be 'imminent' and the term 'reasonably expected to have a direct impact' on the relevant entity.
- We seek further detailed consultation on draft versions of the regulations required under this Part, especially in relation to the undefined term 'turnover threshold' in clause 26(3) and the term 'designated Commonwealth body', to whom these reports must be provided, which is also to be defined by regulation (per clause 8).
- We seek additional consultation prior to the making of any form by the Secretary, or any regulations prescribing how the information is to be provided, as is clearly contemplated under clause 27(4).
- We suggest the reversal of the presumption in clause 28(3), so it will be presumed an entity was acting in 'good faith' in providing the information required under clause 27.
- In accordance with our previous submission, we believe that reporting entities who comply with this section must remain anonymous. This will enhance threat sharing abilities and industry collaboration.²⁰

2.1 The limited use obligation with the National Cyber Security Coordinator (NCSC)

The limited use obligation in relation to reporting information the NCSC is outlined in Part 4 of the Cyber Security Bill. Section 33 provides a summary of this Part, noting that:

Information voluntarily provided under this Part may only be recorded, used and disclosed for limited purposes.

ASFA notes this proposal implements in part Measure 3 from the DHA's Legislative Reforms Consultation Paper.²¹ The other aspects of Measure 3 in relation similar protections with ASD are implemented by Schedule 1 of the Intelligence Services Bill.

The Explanatory Memorandum outlines that:²²

Information that is received by the National Cyber Security Coordinator in the course of a response to a cyber security incident or a significant cyber security incident is considered to be covered by the Limited Use Obligation. Therefore, any information that may be provided in evidence, by the National Cyber Security Coordinator, regarding a cyber security incident which they responded to, is not admissible.

¹⁸ Note – clause 28(1)'s exclusion from liability requires the entity to prove they were acting in good faith under clause 28(3).

¹⁹ The equivalent of 60 civil penalty units, currently set at [\\$313 each](#) but subject to annual change.

²⁰ ASFA, Submission to Home Affairs on the Cybersecurity Legislative Reforms Consultation Paper ([29 February 2024](#)), 3.

²¹ 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper ([December 2023](#)), 18.

²² Explanatory Memorandum, Cyber Security Bill 2024 ([Cth](#)) 68[347].

In considering this Part, regulated entities will need to have regard to the following:

- Clause 35 defines the term ‘significant cyber incident’, for which information may be provided to the NCSC (for all other incidents, see clauses 36 and 39)
- Clause 36 in relation to the ‘voluntary provision of information’ about other incidents which are not ‘significant cyber incidents’ in relation to clause 35.
- Clause 38 outlines the limited use protection covering information provided to the NCSC. These include:
 - the ‘permitted’ uses and disclosures under clause 38(1), which cover assisting an entity to ‘respond to, mitigate or resolve’ a cyber security incident.
 - the restrictions on ‘use and disclosure for civil and regulatory action’ as outlined in clause 38(2).
 - the NCSC can provide the information to other Government agencies and Ministers, if they determine a ‘whole-of-government response’ is necessary.²³
 - the same limited use protection is extended to Commonwealth or State Government entities who obtain information that has been voluntarily provided to the NCSC. They cannot use it for regulatory or enforcement purposes.²⁴
- Clauses 43 and 44 respectively ensure that information covered by the limited use protection is inadmissible in court proceedings and that the NCSC cannot be compelled to appear as a witness in such proceedings.

2.2 ASFA recommendations

In ASFA’s previous submission to DHA, we noted that while we understand the desire to increase information sharing in to combat cyber incidents, the reforms pose several significant challenges, as outlined in **Attachment C**.²⁵

In addition to the concerns expressed there, ASFA recommends further consideration should be given to the following:

- The bill is currently unclear on the difference between a ‘serious cyber incident’, as covered by clause 35, and other cyber incidents, as covered in clauses 36 and 39. Indeed, the bill even expressly contemplates that it may often be ‘unclear’ what type of incident a given set of facts is.²⁶ Therefore, ASFA suggests:
 - It should be made manifestly clear, through express legislative language and in the explanatory memorandum that the limited use protection applies to any information given to the NCSC, not just that relating to ‘serious cyber incidents’.
 - Further detailed guidance needs to be provided in the explanatory memorandum on the differences between serious cyber incidents and non-serious cyber incidents, and which of these need to be reported to the NCSC.
 - The definition of ‘material risk’ in relation to cyber incidents in clause 34 requires further definition, guidance and examples.²⁷

²³ Clause 39(2)(b)-(c).

²⁴ Clause 40(3).

²⁵ ASFA, Submission to Home Affairs on the Cybersecurity Legislative Reforms Consultation Paper ([29 February 2024](#)), 2-4.

²⁶ Clause 36(1)(c).

²⁷ Clause 34(a).

- Further information is also required in relation to the data life cycle for information collected that may be covered by this provision. Including any relevant retention periods and the manner in which the data is to be handled.
- Greater definition should be given to the circumstances in which the NCSC can determine that an incident requires a ‘whole-of-government response.’ There should be an exhaustive list of detailed relevant considerations in the legislation. Without greater clarity on this point, it is unclear when information will be provided by the NCSC to other agencies, as permitted under clause 39. This may hinder collaboration.
- Further regulatory guidance should be provided on how to handle situations where regulated entities may have to engage with third party service providers in relation to these matters. It is unclear how legal liability would work in this context in relation to third parties.
- There should be an express legislative provision that states that no regulatory or enforcement action can be taken where information on a relevant incident has been provided to the NCSC. As the legislation is currently drafted, the information provided to the NCSC cannot be used for that purpose. However, regulators could independently acquire the same information and then take action. It must be clear in the legislation and explanatory materials that where a disclosure has been made under this Part, no regulatory or enforcement action can be taken, regardless of where or how the information is acquired.

3.1 The creation and role of the Cyber Incident Review Board

Part 3 of the Cyber Security Bill creates the Cyber Incident Review Board (the Board) and outlines its functions. A simplified outline of the Board’s role is contained in clause 45, which states:

The Board must cause reviews to be conducted in relation to certain cyber security incidents. The purpose of a review is to make recommendations to government and industry about actions that could be taken to prevent, detect, respond to or minimise the impact of, cyber security incidents of a similar nature in the future.

ASFA notes this proposal implements Measure 4 from the DHA’s Legislative Reforms Consultation Paper.²⁸

The Explanatory Memorandum outlines that:²⁹

Recent high-profile and high-impact cyber security incidents, such as the Optus data breaches in 2022 and 2023, the Medibank data breach in 2022 and the MediSecure data breach in 2024 highlight that government and industry need to do more to effectively learn lessons from cyber security incidents and prepare contingencies for future attacks.

Currently other nations such as the United States have dedicated bodies, such as the Cyber Safety Review Board (CSRB) to review significant cyber security incidents and issuance of public findings. The US’ CSRB has been positively received and has concluded three reviews since its establishment in 2022.

However, there is currently no such similar Commonwealth standing mechanism in Australia that is responsible for undertaking a review of the vulnerabilities that led to a significant cyber security incident, or the effectiveness of the government or industry response to the incident.

²⁸ 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper ([December 2023](#)), 22.

²⁹ Explanatory Memorandum, Cyber Security Bill 2024 ([Cth](#)) 8.

Subject to our recommendations below, ASFA welcomes the creation of the Board as a useful tool to help government and industry learn from past cyber incidents and prepare for future cyber incidents.

3.2 ASFA's recommendations

In respect of the Board, ASFA has the following recommendations:

- For the Board to maintain its independence from government, the Chair should be responsible for the approving the terms of reference of reviews. Further, the Minister should not be empowered to refer an incident to the Board.³⁰
- There should be further consultation in respect of any Rules regulating the Board before they are finalised.³¹
- Clause 49 requires documents sought by the Chair of the Board to be provided within 14 days. Any documents which relate to information otherwise protected under the limited use provisions in Part 4 should be excluded, to protect the confidentiality of that information.³²
- The requirement for the Board to provide draft reports to the Minister should be removed.³³

4.1 The security standards for smart devices

Part 2 of the Cyber Security Bill allows the Rules to provide for security standards for certain 'smart devices' which can directly or indirectly connect to the internet. Clause 12 provides an overview of this Part.

ASFA notes this proposal implements Measure 1 from the DHA's Legislative Reforms Consultation Paper.³⁴

The Explanatory Memorandum outlines that the purpose of this Part is as follows:³⁵

This Part establishes a framework to allow rules to prescribe mandatory security standards for products that can directly or indirectly connect to the internet (relevant connectable devices) that will be acquired in Australia in specified circumstances. The security standards will be complimented through the establishment of obligations on manufacturers to manufacture those products, or comply with other obligations relating to those products, in accordance with the mandatory security standards prescribed.

4.2 ASFA's recommendations

ASFA supports this proposal, subject to further detailed consultation on all aspects of the Rules made under the Cyber Security Bill, as indicated elsewhere in this submission.

All Rules made under the Cyber Security Bill should be subject to the usual provisions for parliamentary oversight and disallowance under the *Legislation Act 2003* (Cth).³⁶

³⁰ Clause 46(1)(a) and 2(c) should be amended accordingly.

³¹ Clause 46(5).

³² If this recommendation is adopted, clauses 56-58 should be amended accordingly.

³³ Clause 51(3)-(5). Clause 54(2)-(3) should also be removed accordingly.

³⁴ 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper ([December 2023](#)), 8.

³⁵ Explanatory Memorandum, Cyber Security Bill 2024 ([Cth](#)) 23[82].

³⁶ [Section 42](#).

B. The SOCI Amendment Bill

5.1 The requirement for data storage systems holding business critical data to be regulated as critical infrastructure assets

Schedule 1 of the SOCI Amendment Bill mandates that data storage systems holding business crucial data should be regulated as critical infrastructure assets under the SOCI Act.

This amends the existing section 9 of the SOCI Act, to insert a new subsection 9(7) which outlines:

*If, under this section, an asset is a critical infrastructure asset, **then a data storage system** in respect of which **all of the following requirements are satisfied** is taken to be **part of the critical infrastructure asset**:*

- a) the responsible entity for the critical infrastructure asset **owns or operates the data storage system**;*
- b) the data storage system is used, or is to be used, **in connection with the critical infrastructure asset**;*
- c) **business critical data** is stored, or is processed in or by, the data storage system (whether or not other information is also stored, or is processed in or, the data storage system);*
- d) for a **hazard** where there is **a material risk** that the occurrence of the hazard could have an impact on the data storage system, there is also a material risk that the occurrence of the hazard could have a relevant impact on the critical 29 infrastructure asset*

ASFA notes this proposal implements Measure 5 from the DHA's Legislative Reforms Consultation Paper.³⁷

The Explanatory Memorandum indicates the purpose of this proposal is as follows:³⁸

*[To] strengthen and standardise obligations across critical infrastructure assets by explicitly outlining that certain data storage systems that hold business critical data do form part of a critical infrastructure asset, regardless of the asset's primary function. The intent of this Schedule is **not to capture all non-operational systems that hold business critical data, only those where vulnerabilities could have a relevant impact on critical infrastructure.***

Examples of the types of systems this could capture include: data storage systems that hold business critical data where there is inadequate network segregation between information and operational technology systems, or data storage systems that hold operational data such as network blueprints, encryption keys, algorithms, operational system code, and tactics, techniques and procedures.

5.2 ASFA's recommendations

In relation to Schedule 1, ASFA seeks more detailed guidance in relation to how the terms 'business critical data', 'hazard' and 'material risk' will be applied in this context. The provision of examples would assist.

We note the term 'business critical data' is defined in [section 5](#) of the SOCI Act.

We also note the term 'critical data storage or processing asset' is defined in [section 12F](#) of the SOCI Act.

³⁷ 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper ([December 2023](#)), 35.

³⁸ Explanatory Memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (Cth) 8[19].

However, these provisions have yet to be interpreted by a court, so guidance with examples would help provide certainty regarding how these provisions are to be interpreted.

Consistent with our previous submission, the phrase ‘information related to any research and development of a critical infrastructure asset’ should be removed from the definition of ‘business critical data’ in section 5 of the SOCI Act. This is because, in the superannuation context, this would include benign demographic and aggregate data used for the modelling of retirement products.³⁹

Consideration should also be given to having sector-specific definitions of ‘business critical data’, rather than one across the board definition, so the unique characteristics of each industry can be handled as necessary.⁴⁰

6.1 The new government consequence management powers, including the power to direct an entity to take action to respond to incidents, not just cyber incidents

Schedule 2 of the SOCI Amendment Bill creates new consequence management powers, whereby Minister may authorize the Secretary to do any of the following under the SOCI Act, as summarised in clause 35AA of the SOCI Amendment Bill:

- give information-gathering directions to regulated entities under (see the existing [section 35AK](#))
- give action directions to regulated entities (see the existing [section 35AQ](#))
- give intervention requests to an authorised agency (see the existing [section 35AX](#)).

The amendments also make it so that these powers do not just apply to ‘cyber incidents’, as is currently the case under the legislation, but to any ‘incident’ more broadly.⁴¹

The amendments also change the current law so that such directions can require a specified entity to disclose information covered by the *Privacy Act 1988* (Cth) (the Privacy Act).⁴²

ASFA notes this proposal implements Measure 6 from the DHA’s Legislative Reforms Consultation Paper.⁴³

These powers are extraordinarily broad. For example, under [section 35AQ](#), the Secretary can:

[G]ive the entity a direction that directs the entity to do, or refrain from doing, a specified act or thing within the period specified in the direction.

The replacement of the narrow term ‘cyber incident’ with the broader term ‘incident’ extends the application of these already extensive powers.⁴⁴

The Explanatory Memorandum notes these changes are necessary because:⁴⁵

The existing limits for utilising a Part 3A power do not adequately consider or address the current threat and risk environment, where an effective response must address noncyber incidents and manage consequential impacts of incidents to other critical infrastructure sector assets. This includes physical incidents like terrorist attacks and natural incidents such as floods or bushfires. The amendments enable use of the framework in response to consequential incidents caused by disruptions to critical infrastructure assets.

³⁹ ASFA, Submission to Home Affairs on the Cybersecurity Legislative Reforms Consultation Paper ([29 February 2024](#)), 5.

⁴⁰ Ibid.

⁴¹ See for example clause 35AB(1)(a) and 35AB(1A)(a).

⁴² Subject to the approval of the Minister administering the Privacy Act, per clause 35AB(9B).

⁴³ 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper ([December 2023](#)), 35.

⁴⁴ Explanatory Memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (Cth) 11[39].

⁴⁵ Ibid 11[37].

6.2 ASFA's recommendations

ASFA cautions against the extension of these already broad powers. ASFA specifically recommends that:

1. Ministerial authorisation of the Secretary giving the directions outlined above should expire after a set timeframe, to ensure that such directions are targeted, limited and subject to appropriate and regular oversight.
2. Ministerial authorisations and directions by the Secretary should be subject to the parliamentary scrutiny and disallowance provisions in the *Legislation Act 2003* (Cth).
3. Consideration should be given as to if these powers should be narrowed, constrained by a more detailed list of legislated necessary preconditions prior to their use.

7.1 The new definition of 'protected information', which includes a harms-based assessment and a non-exhaustive list of relevant factors clarifying when information can be shared or used for other purposes

These changes are contained in Schedule 3 of the SOCI Amendment Bill.

The Explanatory Memorandum outlines that the purpose of these provisions is to:⁴⁶

Introduce a revised, harms-based definition of 'protected information', as well as clarifying disclosure provisions to enable more effective and timely sharing of information under the SOCI Act.

It goes on to explain, as contained in clause 5A that:⁴⁷

The amendments to the definition of 'protected information' clarify that a document or information is only protected information if the disclosure of that document or information could cause harm, or pose risk to the Australian public, the security of the asset, commercial interests, the socioeconomic stability, national security or defence of Australia.

This proposal implements Measure 7 from the DHA's Legislative Reforms Consultation Paper.⁴⁸

7.2 ASFA's recommendations

ASFA recommends that there should be detailed Rules and Guidance outlining the exact circumstances in which employees of the Australian Public Service can disclose otherwise 'protected information' as the terms above are broad and open to myriad interpretations.⁴⁹ These should be subject to further public consultation with industry.

The Limitations on disclosures of protected information should account for the limited use protections which this package proposes to introduce in both the Cyber Security Bill and the Intelligence Services Bill, and ASFA's recommendations in this regard.⁵⁰

ASFA further recommends that clause 5A above should be amended to insert the word 'directly', as emphasised below. All necessary consequential amendments should be made to implement this change, so that:

*[A] document or information is only protected information if the disclosure of that document or information **could is likely to directly** cause harm, or pose risk to the Australian public, the security of the asset, commercial interests, the socioeconomic stability, national security or defence of Australia.*

⁴⁶ Explanatory Memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (Cth) 23[123].

⁴⁷ Ibid, 23[126].

⁴⁸ 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper ([December 2023](#)), 47.

⁴⁹ See for example clauses 42(3) and 42AA.

⁵⁰ Sections 2 and 9 of this submission respectively.

8.1 The new power for the regulator to issue directions to responsible entities to address any serious deficiencies identified in Critical Infrastructure Risk Management Programs (CIRMP)

Schedule 4 of the SOCI Amendment Act the new power for the regulator to issue directions to responsible entities to address any serious deficiencies identified in Critical Infrastructure Risk Management Programs (CIRMP) (Schedule 4).

This proposal implements Measure 8 from the DHA's Legislative Reforms Consultation Paper.⁵¹

The Explanatory Memorandum outlines that the purpose of these amendments is:⁵²

[To] enable the regulator to issue directions to address any serious deficiencies that are identified in a critical infrastructure risk management program (CIRMP) held by a responsible entity as part of obligations under Part 2A of the SOCI Act. The ability for the regulator to issue such a direction will help ensure that CIRMP obligations achieve the intent of embedding preparation, prevention, and mitigation activities into the business-as-usual operations of critical infrastructure assets.

Powers to make directions are given to the Secretary, or any other 'relevant official', under clause 30AI(1)-(2).

The term, 'serious deficiency' is defined under clause 30AI(3) as any deficiency posing a material risk to 'national security', 'the defence of Australia' or 'the social or economic stability of Australia or its people.'

The regulated entity must comply with the direction, subject to a civil penalty of up to \$78,250.⁵³

8.2 ASFA's recommendations

ASFA recommends the following in relation to Schedule 4:

1. The class of 'relevant officials' capable of issuing a direction under this part should be simplified to just 'the Secretary or their authorised delegate.'⁵⁴ The current longer list confers this significant power on too many potential individuals.
2. Further guidance needs to be provided on examples of the kinds of situations which would constitute a 'serious deficiency', as outlined above, because the legislative language could cover a multitude of scenarios. This should be narrowed.
3. The Regulator should be defined in the legislation, so it is clear who will be the responsible entity in respect of this clause.

⁵¹ 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper ([December 2023](#)), 51.

⁵² Explanatory Memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (Cth) 35[213].

⁵³ Clause 30AI(5) specifies a maximum of 250 penalty units of up to [\\$313 each](#).

⁵⁴ Clause 30AI(2).

C. The Intelligence Services Bill

9.1 The new limited use obligation protecting information voluntarily given to the ASD during an impacted entity's engagement on a cyber incident to complement Part 4 of the Cyber Security Bill.

Schedule 1 of the Intelligence Services Bill implements a limited use protection like that in Part 4 of the Cyber Security Bill, except this reform relates to information shared with the ASD, not the NCSC.

The provisions of this Bill operate in a substantially similar manner to the amendments in Part 4 of the Cyber Security Bill. That is:

- Clause 41BA limits the use and communication of certain cyber security information received by ASD.
- Clause 41BB outlines the purposes for which that information can be communicated, which are like those in the Cyber Security Bill.
- Clause 41BC limits the use of information received by third parties under clause 41BB.
- Clause 41BF and 41BG respectively make this information inadmissible in legal proceedings and bar the Director-General or ASD staff from being compelled as witnesses in such proceedings.

9.2 ASFA's recommendations

ASFA's recommendations regarding the limited use protections in the Cyber Security Bill in relation the NCSC, apply equally to this proposal, as it replicates similar provisions regarding the ASD.⁵⁵

⁵⁵ See pages 8-9 of this submission.

The Cyber Security Legislative Package 2024

Summary of the key changes in the Cyber Security Package 2024

1. [The Cyber Bill](#)

1. Mandatory Ransomware Reporting (Part 3, EM – Page 39)	Section 25 provides the simplified outline of Part 3 of the Act. The simplified outline for this Part establishes a reporting obligation which is imposed on certain entities who are impacted by a cyber security incident, and who have provided or are aware that another entity has provided, a payment or benefit (which is referred to as a ransomware payment) to an entity that is seeking to benefit from the impact or the cyber security incident. In this Part, under section 27, particular information must be included in a ransomware payment report, including information relating to the cyber security incident, the demand made by the extorting entity and the ransomware payment.
2. Limited Use Obligation with the National Cyber Security Co-ordinator (Part 4, EM - Page 56)	Section 33 provides a simplified outline for Part 4 of this Act. The opening sentence of the simplified outline provides guidance to the reader to the effect that information may be voluntarily provided to the National Cyber Security Coordinator in relation to significant cyber security incidents and sets out the parameters for the record, use and disclosure of information voluntarily provided under this Part.
3. Cyber Incident Review Board (Part 5, EM – Page 70)	Section 45 provides a simplified outline for Part 5 of this Act. The opening sentence of the simplified outline provides guidance to the reader to the effect that Part 5 establishes the Cyber Incident Review Board (the Board). The Board must cause reviews to be conducted in relation to certain cyber security incidents. The purpose of the Board undertaking a review is to make

	<p>recommendations to government and industry about actions that could be taken to prevent, detect, respond to or minimise the impact of cyber security incidents of a similar nature in the future.</p>
<p>4. Security Standards for Smart Devices (Part 2, EM – Page 23)</p>	<p>This Part establishes a framework to allow rules to prescribe mandatory security standards for products that can directly or indirectly connect to the internet (relevant connectable devices) that will be acquired in Australia in specified circumstances. The security standards will be complimented through the establishment of obligations on manufacturers to manufacture those products, or comply with other obligations relating to those products, in accordance with the mandatory security standards prescribed.</p>

2. The SOCI Amendment Bill

<p>1. Data storage systems holding business critical data to be regulated as critical infrastructure assets (Schedule 1, EM - Page 7)</p>	<p>The SOCI Act currently imposes positive security obligations on data storage and processing assets, where this is the primary function of the critical infrastructure asset. However, these obligations do not extend to the adequate protection of secondary systems related to other classes of critical infrastructure assets that hold ‘business critical data’.</p> <p>The purpose of the amendments contained within this Schedule are to strengthen and standardise obligations across critical infrastructure assets by explicitly outlining that certain data storage systems that hold business critical data do form part of a critical infrastructure asset, regardless of the asset’s primary function. The intent of this Schedule is not to capture all non-operational systems that hold business critical data, only those where vulnerabilities could have a relevant impact on critical infrastructure. Examples</p>
--	--

	<p>of the types of systems this could capture include: data storage systems that hold business critical data where there is inadequate network segregation between information and operational technology systems, or data storage systems that hold operational data such as network blueprints, encryption keys, algorithms, operational system code, and tactics, techniques and procedures.</p>
<p>2. New government consequence management powers - to direct an entity to take action to respond to incidents, beyond cyber incidents (Schedule 2, EM – Page 11)</p>	<p>The purpose of the amendments contained within this Schedule is to facilitate management of multi-asset incidents and their consequences through the existing government assistance framework in Part 3A of the SOCI Act. Incidents in scope could be natural or man-made, so long as they impact the availability, integrity and reliability of the critical infrastructure asset. This includes incidents from all types of hazards, such as cyber and information hazards, physical and natural hazards, personnel hazards, and supply chain hazards.</p> <p>To achieve this outcome, the amendments to Part 3A shift the language from purely referencing a ‘cyber security incident’ to an ‘incident’ more broadly, for information gathering and action directions only, whilst maintaining the criteria that the incident has had, is having, or is likely to have, a relevant impact on one or more critical infrastructure assets.</p>
<p>3. New definition of ‘protected information’. A harms-based assessment and a non-exhaustive list of relevant information and clarifies when protected information can be shared/used for other purposes (Schedule 3, EM – Page 23)</p>	<p>The amendments made by Schedule 3 will introduce a revised, harms-based definition of ‘protected information’, as well as clarifying disclosure provisions to enable more effective and timely sharing of information under the SOCI Act.</p> <p>The current protected information provisions under the SOCI Act were designed to apply similar information sharing restrictions on private entities operating critical infrastructure to those imposed on public service employees.</p>

	<p>However, feedback from all levels of government and industry has demonstrated that the SOCI Act may, in some instances, unnecessarily limit the ability of Government, responsible entities and their employees to use or disclose information in the course of ordinary business, or mitigate relevant risk effectively. These limitations have the effect of hobbling the response to high risk or time sensitive events.</p> <p>The amendments to the definition of ‘protected information’ clarify that a document or information is only protected information if the disclosure of that document or information could cause harm, or pose risk to the Australian public, the security of the asset, commercial interests, the socioeconomic stability, national security or defence of Australia.</p> <p>Clarity for entities on what information is protected information and where disclosure may be authorised will provide greater confidence in the use and disclosure of protected information, limit disruption and the regulatory burden on entities, and facilitate broader security uplift through collaboration between industry and government.</p>
<p>4. New power for the regulator to issue directions to a responsible entity to address any serious deficiencies that are identified in a critical infrastructure risk management program (Schedule 4, EM – Page 35)</p>	<p>The amendments in Schedule 4 address gaps in the powers available to regulators to enforce critical infrastructure risk management obligations.</p> <p>Specifically, these amendments will enable the regulator to issue directions to address any serious deficiencies that are identified in a critical infrastructure risk management program (CIRMP) held by a responsible entity as part of obligations under Part 2A of the SOCI Act. The ability for the regulator to issue such a direction will help ensure that CIRMP obligations achieve the intent of</p>

	<p>embedding preparation, prevention, and mitigation activities into the business-as-usual operations of critical infrastructure assets.</p> <p>The intention is that where deficiencies are identified, these directions would be issued in accordance with the Cyber and Infrastructure Security Centre's (CISC) Compliance and Enforcement Strategy. Wherever possible, the CISC seeks to work in partnership with industry to ensure regulated entities understand and effectively manage their risks, reserving compliance levers as last resort measures.</p>
--	---

3. [The IS Bill](#)

<p>A limited use obligation protecting information voluntarily given to the Australian Signals Directorate during an impacted entity's engagement on a cyber incident to complement Part 4 of the Cyber Bill.</p>	<p>See Schedule 1 and EM – Page 7.</p>
---	--



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 \(homeaffairs.gov.au\)](https://www.homeaffairs.gov.au/cyber-security-legislation-reforms)

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 35AC¹ 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 234³, 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 234⁵ 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 234⁶ 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.

An 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 utilising 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

Yours sincerely

Mary Delahunty
Chief Executive Officer