SUBMISSION

Cyber Security Legislative Package – Consultation on Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act)

14 February 2025

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: 2025/05

Ashley Bell
Assistant Secretary – Cyber Policy and Programs Branch
Department of Home Affairs
6 Chan St, Belconnen ACT 2617
Via email: pjcis@aph.gov.au

14 February 2025

Dear Mr Bell,

Cyber Security Legislative Package – Consultation on Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act)[1]

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission in response to this consultation by the Department of Home Affairs (DHA).

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.

We unite the superannuation community, supporting our members with research, advocacy, education and collaboration to help Australians enjoy a dignified retirement. We promote effective practice and advocate for efficiency, sustainability and trust in our world-class retirement income system.

ASFA's Opening Comments

ASFA supports the Cyber Security Legislative Package 2024.

We note that these reforms have been the product of significant consultation, following:

1. The release of the *2023-2030 National Cyber Security Strategy* on 22 November 2023.
2. The *Cyber Security Legislative Reforms Consultation Paper*, to which ASFA made a submission in February 2024.
3. The introduction of the Cyber Security Legislative Package to Parliament, by the Minister for Home Affairs and Cyber Security, the Hon. Tony Burke MP on 9 October 2024.
4. The review of that Legislation by the Parliamentary Joint Committee on Intelligence and Security between 10 October 2024 and 18 November 2024, with the Committee's report available here.

[1] Hereafter, this consultation package is referred to as the Rules under the Cyber Security Legislative Package 2024.

ASFA welcomes the fact that the Committee's report on the Cyber Security Legislative Package referenced ASFA's submission nine times, including making a number of recommendations which reflected feedback from ASFA, such as:[2]

- **Recommendation 2** - The Australian Government [should] ensure that ransomware reporting mechanisms are as user friendly and accessible as possible for the range of businesses subject to the Cyber Security Bill 2024's reporting obligations, and that the Australian Government continues to prioritise work to **minimise duplication in cyber security incident reporting requirements for all businesses**.[3]

- **Recommendation 3 -** The Australian Government [should] ensure that the **Department of Home Affairs and the Australian Signals Directorate are given adequate resources to educate businesses** about the proposed ransomware reporting obligations and to provide **clear guidance on interpretation of the legislation**.[4]

- **Recommendation** 7 - The Committee recommends the protections conferred by the 'limited use' provisions be more clearly expressed in the Cyber Security Bill 2024 and the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024 and associated explanatory memoranda, and **that the Department of Home Affairs develop guidance to ensure they are well understood by industry.**[5]

- **Recommendation 8 -** The Committee recommends that the Cyber Security Bill 2024 and the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024 be amended to make clearer that:

    - disclosure of information under the ransomware reporting obligation **does not amount to a subsequent waiver of legal professional privilege**; and

    - the provisions **do not limit or affect any right, privilege or immunity** that the reporting entity has in respect to any proceeding.[6]

This detailed engagement with the legislation demonstrates ASFA's commitment to working constructively with Government to ensure that industry and all stakeholders clearly understand and comply with their cyber security obligations.

ASFA strongly agrees with Minister Burke, who has said these reforms are required to:

> *[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.*

[2] Recommendations are taken from the Parliamentary Joint Committee on Intelligence and Security's Advisory Report (18 November 2024) at xiii to xiv.
[3] See recommendations from ASFA's submission of 25 October 2024 at 9-10.
[4] See recommendations from ASFA's submission of 25 October 2024 at 11, 14 and 16-17.
[5] See recommendations from ASFA's submission of 25 October 2024 at 11-12.
[6] Ibid.

ASFA's submission in relation to this consultation on the rules is structured as follows:

1. **Appendix A** will provide our specific recommendations in relation to the rules outlined below, as not all the package is equally relevant to the superannuation sector. Our comments focus on:
    - The Cyber Security (Ransomware Reporting) Rules 2024.[7]
    - The Security of Critical Infrastructure (Critical infrastructure risk management program) Amendment (Data Storage Systems) Rules 2024 (Data Storage Systems Rules).[8]
    - The Cyber Security (Cyber Incident Review Board) Rules 2024.[9]
2. For the Department's convenience, ASFA also provides in **Appendix B** our October 2024 submission to the Parliamentary Joint Committee on Intelligence and Security, so that you may review our position on the Cyber Security Legislative Package as a whole. **Appendix B** also provides detailed information on the activities ASFA has undertaken to combat all forms of financial crime, including cybercrime, through our Financial Crime Protection Initiative, announced in September 2024. We would be happy to brief DHA on this further at your convenience.

Subject to the caveats expressed in [1] and [2] above, ASFA supports the Cyber Security Legislative Package, and thanks the Department for your engagement on these important issues.

Should you wish to discuss these matters further, please feel free to reach out to ASFA Senior Policy Adviser, Sebastian Reinehr at sreinehr@superannuation.asn.au or on 0474 704 992.

Thank you in advance for your consideration.

Yours sincerely

James Koval

Head of Policy and Advocacy

[7] Hereafter referred to as the Ransomware Reporting Rules 2024.
[8] Hereafter referred to as the Data Storage System Rules.
[9] Hereafter referred to as the Cyber Incident Review Board Rules.

Appendix A - ASFA's Specific Recommendations on the Rules

General Recommendations

As an overarching recommendation, ASFA recommends that DHA expedite the implementation of recommendations 3 and 7 of the Parliamentary Committee on Intelligence and Security's report, as outlined above. That is, the Department should move with all deliberate speed to undertake the following:

- **Recommendation 3 -** The Department of Home Affairs and the Australian Signals Directorate are given adequate resources to **educate businesses about the proposed ransomware reporting obligations and to provide clear guidance on interpretation of the legislation**.[10]

- **Recommendation** 7 - The Committee recommends the protections conferred by the 'limited use' provisions be more clearly expressed in the Cyber Security Bill 2024 and the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024 and associated explanatory memoranda, and **DHA should develop guidance to ensure they are well understood by industry**.[11]

Regarding to the most relevant rules for the superannuation sector, ASFA provides the following specific recommendations:

The Ransomware Reporting Rules

Recommendation 1 - ASFA supports clarification in section 4 of the rules that the definition in the rules adopt the following terms from the primary legislation

- cyber security incident (section 9 of the Act)
- ransomware payment (section 26(1) of the Act)
- reporting business entity (section 26(2) of the Act)

Recommendation 2 - The recommendation which follows is the most important of all ASFA's specific recommendations on these rules.

ASFA recommends that section 5(c) of the rules should be amended to provide clarity over reporting obligations when ransomware payments are made by third parties on behalf of a regulated entity.

Section 5(c) currently reads as follows:

> *Part 3 of the Cyber Security Act imposes an obligation to provide a ransomware payment report if an entity:*
>
> *(a) is a reporting business entity;* ***and***
>
> *(b) is impacted by a cyber security incident;* ***and***
>
> *(c)* ***has provided, or is aware that another entity has provided on their behalf****, a ransomware payment to an entity that is seeking to benefit from the impact or the cyber security incident.*

[10] See recommendations from ASFA's submission of 25 October 24 at 11, 14 and 16-17.
[11] See recommendations from ASFA's submission of 25 October 2024 at 11-12.

The feedback received by ASFA is that how this would currently be interpreted is unclear in the context of cyber-attacks on third-party suppliers. For example, if a vendor has paid a ransom in relation to information assets that include information assets belonging to another regulated entity (such as a superannuation fund), would the fund have to report or would their vendor?

It is currently unclear if this applies whenever a third party who interacts with a regulated entity, such as a superannuation fund, makes a ransomware payment. Or alternatively, if superannuation funds only obligated to report when they instruct a third-party vendor to make a payment.

ASFA therefore recommends that greater clarity be provided on how this regulation is to be interpreted through the explanatory materials. ASFA further recommends that the better interpretation would be that superannuation funds would only have to report ransomware payments made by third parties on their behalf if they specifically requested for that done by the third party on their behalf.

Conversely, where third parties happen to hold data and choose to make a payment without a specific request from a fund, superannuation funds should not be required to report this as, given the complexity of supply chains involved, it could lead to unnecessary duplication, over-reporting or a lack of clarity about where the reporting obligation lies.

Recommendation 3 - ASFA supports section 7 of the rules, which clarifies what information must be provided in a ransomware payment report under section 27(2) of the Cyber Security Act 2024 (Cth).

The Data Storage System Rules

Recommendation 4 - ASFA welcomes the clarification provided in section 3 of these rules that makes it expressly clear that the following expressions used in this instrument are defined in the SOCI Act, including:

a. business critical data (section 5)
b. critical component (section 5)
c. critical infrastructure asset (section 9)
d. critical hospital (section 5)
e. critical worker (section 5)
f. relevant impact (section 8G)
g. responsible entity (section 12L)
h. security (section 5).

Recommendation 5 - ASFA notes these rules make changes to the definition of material risk, At the end of section 6 of the SOCI CRIMP Rules 2023, which defines the criteria for 'material risk' under section 30AH(8) of the SOCI Act.

These rules add the following additional limb (f) to the term material risk:

> *(f) impact to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data*

ASFA seeks clarification from DHA as to why this change was required.

The Cyber Incident Review Board Rules

Recommendation 6 - ASFA supports the clarification in section 4 of the rules that the following terms from the Act have the same meaning in this instrument:

- Cyber Incident Review Board (section 60)
- Cyber Security Incident (section 9)
- Expert Panel (section 70)

Recommendation 7 - Section 7 of the rules requires the Board to 'consider' a referral made to it under section 46 of the Act.

ASFA recommends this should be amended to make clear that unless a referral is 'considered' within 30 calendar days, and a decision made by the Board regarding whether (or not) to pursue the referral, the referral should lapse and be of no further effect.

Furthermore, during the consideration period for a referral, the Board should ensure that such referrals remain private.

This minor adjustment would ensure expeditious decision making and fairness to the parties subject to a referral by removing the threat of prolonged, public referrals upon which no decision has been made.

This is desirable as a referral may imply misconduct, even where none exists.[12]

Recommendation 8 - Section 8 of the rules outlines that, when considering and prioritising referrals for review, the Board must have regard to:

*(a) the **severity and scale of impact** of the cyber security incidents to which those referrals and reviews relate (as mentioned in subsection 46(2) of the Act)*

ASFA recommends that some standardized metrics for assessing '**severity, scale and impact'** should be established by the Board and published for public consultation. This will help to ensure that the terms are applied consistently and objectively across all cyber incidents.

Recommendation 9 - ASFA recommends that section 14 should be amended so that appointments to the Board are overseen by the Chair of the Board, not the Minister.

This would better maintain the independence of the Board from government. All other sections of the regulations requiring disclosures to the Minister should also be amended so that such disclosures are made to the Chair of the Board, not the Minister.

Recommendation 10 - ASFA recommends that, to maintain the independence of the Board from government, section 20 should be amended so that members can only be removed by the Chair of the Board and not by the Minister. Or, where the Chair is the person subject to potential removal, this should require a majority vote of all Board Members.

[12] Similar considerations apply in relation to section 11 of the rules, which requires public notification of the existence of a review once a decision has been made in relation to a referral. Consideration should be given to whether it may be more appropriate for reviews to be conducted privately prior to a final report being compiled which can holistically analyse the relevant circumstances, without causing damage to public reputation or unduly prejudicing other legal proceedings.

Appendix B – ASFA's Submission the Parliamentary Joint Committee on Intelligence and Security's Advisory Report on the Cyber Security Legislative Package 2024

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: [13]

> *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.*

[13] *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: [14]

> *[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:[15]

> *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 Act[16]
2. the reporting of ransomware incidents[17]
3. measures designed to increase engagement with the National Cyber Security Coordinator (NCSC) and Australian Signals Directorate (ASD) during cyber incidents[18]
4. amendments to the SOCI Act regarding data storage systems and business critical data[19]
5. additional powers for the Government to review and remedy serious deficiencies in Critical Infrastructure Risk Management Plans.[20]

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

[14] *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).
[15] ASFA, Submission to Home Affairs on the Cybersecurity Legislative Reforms Consultation Paper (29 February 2024), 2.
[16] 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.
[17] Ibid, 3. This is dealt with in Part 3 of the Cyber Security Bill in this package.
[18] 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.
[19] Ibid, 4-8. This is dealt with in Schedule 1 of the SOCI Amendment Bill in this package.
[20] 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**.[21]

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:[22]

    > *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:[23]

    > *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.

---

[21] ASFA, Submission to Home Affairs on the Cybersecurity Legislative Reforms Consultation Paper, 2 (29 February 2024)
[22] ASFA, Submission to Treasury on the Scams Prevention Framework – Exposure Draft Legislation (4 October 2024).
[23] *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, Sebastian Reinehr, at sreinehr@superannuation.asn.au or 0474 704 992, 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

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.[24]

The Explanatory Memorandum outlines that:[25]

> *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.[26]
    - the entity must be aware of a 'demand' made by the 'extorting entity' that would cause them to 'benefit' from the incident.[27]
    - 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.[28]
    - 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.[29]
    - 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.

[24] 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (December 2023), 16.
[25] Explanatory Memorandum, Cyber Security Bill 2024 (Cth) 39[178].
[26] Clause 26(1)(a)-(c). Please note, the term 'cyber incident' is defined is clause 10 and this should be read alongside the presumption in clause 26(4).
[27] Clause 26(1)(d).
[28] Clause 26(1)(e).
[29] 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.[30]

Regulated entities that fail to report ransomware payments in accordance with this Part could lead to civil penalties of $18,780.[31]

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 property 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.[32]

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.[33] 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:[34]

> *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.*

---

[30] Note – clause 28(1)'s exclusion from liability requires the entity to prove they were acting in good faith under clause 28(3).
[31] The equivalent of 60 civil penalty units, currently set at $313 each but subject to annual change.
[32] ASFA, Submission to Home Affairs on the Cybersecurity Legislative Reforms Consultation Paper (29 February 2024), 3.
[33] 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (December 2023), 18.
[34] 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.[35]
  - 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.[36]

- 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**.[37]

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.[38] 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.[39]

[35] Clause 39(2)(b)-(c).
[36] Clause 40(3).
[37] ASFA, Submission to Home Affairs on the Cybersecurity Legislative Reforms Consultation Paper (29 February 2024), 2-4.
[38] Clause 36(1)(c).
[39] 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.[40]

The Explanatory Memorandum outlines that:[41]

> *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.*

[40] 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (December 2023), 22.
[41] 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.[42]

- There should be further consultation in respect of any Rules regulating the Board before they are finalised.[43]

- 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.[44]

- The requirement for the Board to provide draft reports to the Minister should be removed.[45]

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.[46]

The Explanatory Memorandum outlines that the purpose of this Part is as follows: [47]

> *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).[48]

---

[42] Clause 46(1)(a) and 2(c) should be amended accordingly.
[43] Clause 46(5).
[44] If this recommendation is adopted, clauses 56-58 should be amended accordingly.
[45] Clause 51(3)-(5). Clause 54(2)-(3) should also be removed accordingly.
[46] 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (December 2023), 8.
[47] Explanatory Memorandum, Cyber Security Bill 2024 (Cth) 23[82].
[48] 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.[49]

The Explanatory Memorandum indicates the purpose of this proposal is as follows:[50]

> ***[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.

[49] 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (December 2023), 35.
[50] 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.[51]

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.[52]

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.[53]

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).[54]

ASFA notes this proposal implements Measure 6 from the DHA's Legislative Reforms Consultation Paper.[55]

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.[56]

The Explanatory Memorandum notes these changes are necessary because:[57]

> *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.*

---

[51] ASFA, Submission to Home Affairs on the Cybersecurity Legislative Reforms Consultation Paper (29 February 2024), 5.
[52] Ibid.
[53] See for example clause 35AB(1)(a) and 35AB(1A)(a).
[54] Subject to the approval of the Minister administering the Privacy Act, per clause 35AB(9B).
[55] 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (December 2023), 35.
[56] Explanatory Memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (Cth) 11[39].
[57] 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:[58]

> *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:[59]

> *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.[60]

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.[61] 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.[62]

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.*

---

[58] Explanatory Memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (Cth) 23[123].
[59] Ibid, 23[126].
[60] 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (December 2023), 47.
[61] See for example clauses 42(3) and 42AA.
[62] 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.[63]

The Explanatory Memorandum outlines that the purpose of these amendments is:[64]

> *[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.[65]

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.'[66] 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.

[63] 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper (December 2023), 51.
[64] Explanatory Memorandum, Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (Cth) 35[213].
[65] Clause 30AI(5) specifies a maximum of 250 penalty units of up $313 each.
[66] 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.[67]

[67] See pages 8-9 of this submission.