Australian Banking Association

2023 – 2030 Cyber Security Strategy: Legislative Reforms

Consultation Paper

1 March 2024

Australian Banking Association

Table of Contents

Australian Banking Association

Key recommendations

The ABA welcomes the consultation on proposed reforms to support the 2030 Cybersecurity Strategy and is grateful for the opportunity to provide input. The Banking Industry stands as a willing and enthusiastic partner in fortifying Australia's cybersecurity landscape. As the organisations entrusted with the safeguarding of Australians' financial assets, banks are acutely aware of the significance of cybersecurity risk management and the evolving capabilities required to address current and emerging risks.

The ABA supports the intent behind the proposed reforms to further enhance collaboration between industry and government in the cybersecurity domain as well as strengthen shared understanding of the nature and possible responses to cyber security threats. However, any reforms must be considered carefully to ensure that they do not have the unintended consequence of distracting attention and resources away from the actual management of a cyber security incident or diverting resources into the development of compliance systems and processes rather than in actual cyber defences.

The consultation addresses a broad range of reforms. For relevance the ABA has limited its response to *Measures 2 – 8*, with certain questions grouped together so that responses address these questions thematically. In addition to the detail already provided in the consultation paper, the ABA recommends additional consideration be given to the below themes which are further detailed in responses to the proposals.

- Greater granularity on the problems/gaps in the current landscape and how the proposed reforms address those.
- Consideration of how the scope and requirements can be limited to an appropriate minimum level – meeting the objective of the proposals while avoiding unnecessary risk and complexity.
- Consideration of existing regulatory and reporting regimes – including how these intersect with proposals and where they could be simplified.
- Clarity on the intended limitation of certain measures and the expected residual risk entities would be required to assume.

With specific reference to the banking industry, the ABA urges particular attention be paid to the substantial existing regulation and the significant overlap between incumbent regulation and the proposed measures. Cybersecurity and information security risks in the banking sector are already comprehensively managed, primarily by, but not limited to, the SOCI Act and Prudential Standards (e.g., CPS 234).

While further discussion on any perceived gaps is welcomed, the ABA in principle strongly urges that any proposed reforms avoid introducing duplicative obligations, and desired outcomes are met within the incumbent regulatory landscape. Where obligations are introduced agnostic to existing regulation, the impacts of unintended complexity and conflicting requirements can be material.

Overlapping regulation is unlikely to be solely a challenge in the banking sector, suggesting that greater nuance in the sector-by-sector requirements may be required. The ABA acknowledges the importance of getting these reforms right and is eager to support the Government in ensuring the proposed reforms are as effective as possible.

Policy Director contact: Maxwell Pryor

Policy Director

[redacted]

About the ABA

The Australian Banking Association advocates for a strong, competitive, and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

Australian Banking Association

ABA Submission to consultation questions

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

8. What mandatory information, if any, should be reported if an entity has been subject to a ransomware or cyber extortion incident?

9. What additional mandatory information should be reported if a payment is made?

10. What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats, whilst minimising the regulatory burden on entities with less capacity to fulfil these obligations?

The ABA supports the intent of *Measure 2* – to facilitate improved quality and quantity of information sharing to uplift responsiveness, mitigation, and resilience. However, it is critical to ensure that any new regime both minimises inclusion of sensitive/legally protected information and does not unreasonably burden businesses with reporting obligations, particularly during an incident. In particular, the ABA urges consideration of the following:

Information requirements

Based on the proposed reforms and the ABA's engagement with Home Affairs to date, it appears that the anticipated information to be provided extends well beyond whether a ransom payment has been made and to whom. Certain categories of information of a commercially sensitive/proprietary nature or those subject/likely to be subject to legal privilege (e.g., indicators of compromise, root cause analysis, impacts on the organisation etc.) do not appear to have a compelling prima facie case for inclusion in reporting – particularly where a ransomware payment has not been made. While it is acknowledged that some of this information may have relevance, the ABA is concerned incremental risk introduced to entities by requiring the provision of highly sensitive information (without a strong case for its utility) may disincentivise engagement with the regime.

The ABA recommends that Government ensure that information is only collected where there is a clear basis that the information will help mitigate ransomware threats. The ABA additionally seeks further detail on the alignment of the proposed information gathering processes and usage to existing threat intelligence gathering programs (e.g. CISO Lens).

Duplicative reporting

Whilst acknowledging that the proposals apply economy-wide to address variances in obligations across entities and industries, the ABA believes thorough consideration of potential overlap between existing and proposed obligations is required, particularly for highly regulated industries.

The below highlights some examples of existing regulation that applies to the banking industry already and has the potential for duplication with *Measure 2*.

- Critical infrastructure owners are already subject to mandatory incident reporting obligations. Covered assets (*Section 5*) are broad, covering much of the economy.
- Ransomware is captured as a 'cyber security incident' in legislation[1] and the required reporting and engagement with government is broad.
- Prudentially regulated entities (i.e. banks, superannuation funds etc.) are subject to further information security obligations under CPS 234.

[1] Section 12M, Security Legislation Amendment (Critical Infrastructure) Act 2021

The ABA recognises that Home Affairs is alive to these concerns and welcomes the acknowledgement of these issues via the suggested exemption for SOCI regulated entities from the first report. However, it is difficult to see why retaining the second report for critical infrastructure is warranted given any ransom payment would likely be captured by an entity's response.[2] Additionally, there is a risk that obligations that are not designed with a holistic approach will risk establishing duplicative regimes. Requiring the second report for SOCI Act regulated entities would effectively subject them to two separate reporting regimes for ransomware (one under SOCI for an incident and a second under the ransomware regime if a payment were to be made).

The ABA suggests parallel consideration of opportunities to simplify the existing reporting regime. There are concerns that additional complexity may unintentionally obstruct an entity's ability to respond to the immediate technical and customer impacts of the incident. It is noted that Home Affairs has provided a commitment to additional consultation on simplification of reporting[3]. The banking industry welcomes this and looks forward to engaging with the process while noting that new ransomware reporting may be most effective if launched concurrently with identified simplified processes emerging from this consultation.

Materiality threshold

The ABA urges that a clear materiality threshold and taxonomy for incident reporting is established to set defined limitations on reporting to serious/legitimate ransomware attacks only. It is recommended that this threshold is developed with industry discussion, ensuring that reportable incidents are those that are sufficiently serious to warrant reporting, and that guidance on this threshold is detailed enough to remove ambiguity. Guidance provided should additionally clearly delineate between reportable and non-reportable incidents (e.g. when would thwarted ransomware attacks need to be reported?).

There are comparative regimes globally that have sought to minimise both risk in sharing information, and duplicative reporting. For example, the US ransomware reporting regime includes protections for information subject to legal professional privilege and excludes the operation of the freedom of information regime. The US also provides a reference point for duplicative reporting via the 'substantially similar reported information' exemption contained in the US Cyber Incident Reporting for Critical Infrastructure Act of 2022 which reduces duplicative reporting where an entity provides similar information to other Federal Agencies.

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

The ABA appreciates the intent of limiting reporting obligations to larger businesses – reducing the impact on SMEs with less capacity to meet compliance requirements while focusing on businesses that can more readily comply, provide higher quality reporting, and may be more attractive targets. While the ABA does not take a position on specific turnover thresholds, consideration of the following is urged when determining whether the binary reporting threshold meets the objectives of ransomware reporting:

- As customers of the banks, incidents affecting small businesses can indirectly affect the banking industry more broadly. Thus, greater visibility may have a multiplier benefit beyond the reporting entities, supporting risk mitigation.

[2] Section 12P, Security Legislation Amendment (Critical Infrastructure) Act 2021
[3] Footnote 3, page 14 – Consultation paper

- Smaller businesses (<$10m turnover) are often those with less capacity and resources to prevent cybercrime vs larger entities, and therefore theoretically benefit the most from greater government visibility of ransomware attacks.
- Given their capability and numerical quantity, we would expect smaller businesses to represent almost all ransomware attacks (at least their natural share of 98.3%)[4]. It's unclear how both the quantity of attacks against this group, and the potential for different mixes of attacks would be addressed in this reporting.
- Deliberate exclusion of businesses by turnover may perversely make them a more attractive target for criminals.

In addition to business turnover, the ABA recommends consideration be given to whether specific turnover agnostic categories of companies should be established. As certain smaller vendors exist within critical infrastructure supply chains and support business critical processes, turnover based omission from reporting obligations would likely present an unacceptable intelligence gap and disproportionately incentivise threat actors to target these entities – potentially as a back door into larger entities. Fundamentally, these categories would reflect the likelihood that attacks on certain small entities would still present a risk to critical infrastructure irrespective of the entity's turnover.

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

Required time periods for reporting should be reflective of the intent of the regime. As it does not appear that in-incident triaging is the express intent of ransomware reporting, timelines should prioritise alignment to other reporting while minimising the imposition of obligations during the immediate response to an incident.

The ABA urges consideration of existing reporting obligations, including the proposed Notifiable Data Breach (NDB) reporting timeframe (72 hours) in the Privacy Act, and the existing 72-hour mandatory incident reporting mechanism in the SOCI Act. It's possible that when setting a relatively prompt reporting timeline (e.g. 72 hours) that the required information may not be available and/or not be fully formed. Reporting procedures should be sufficiently flexible to enable extended timeframes for such information, and the ability to retrospectively modify information provided. The ABA recommends further consideration of how best to balance notification speed and the quality of information that may be available at the earliest stages of an investigation into an attack.

13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?

14. How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

In principle, no-fault and no-liability principles should provide greater confidence to entities reporting a ransomware or cyber extorsion incident. However, there is significant ambiguity how these principles would work in practice, with further clarity required to determine what degree of confidence they may confer upon entities. In particular:

- It is unclear as to the extent that the no-liability principle would constitute a defence to any breaches of sanctions laws or instruments of crime laws arising from a ransom payment.
- Legislative clarity is required regarding the limits of confidentiality and how this information could be used and shared across Government.

[4] Consultation paper page 15: businesses above $10m in turnover represent 1.7% of total businesses

- It is unclear how information provided under this proposal would interact with legal professional privilege and the Freedom of Information regime.

While the intent of the proposal is acknowledged, ultimately, greater detail as to what relief the no-liability model provides, including its limitations, is required to make any meaningful assessment. Where relief is not the intent of the proposal it should be made abundantly clear, as it is unlikely that the no-liability regime would tangibly improve confidence to report what is otherwise an extremely complex situation. The ABA recommends that the appropriateness of existing accountability models is assessed in tandem with the no-liability regime. For example, in financial services and banking the Corporations Act addresses failures in cyber risk management, reflected in case law[5] and Director's Duties requiring management of cybersecurity risks).

Furthermore, the extent that information is anonymised and aggregated will also drive industry confidence. For example, confidence could be improved through a confirmation that Government will only share information at a summarised level, which crucially ensures that both the entity and action taken to resolve the incident cannot be identified. It is expected that the timing of any public release of information could itself lead to entity identification. As such, it is recommended that any reporting adopts a consistent cadence in both publication, and sufficient lead time between incident and publication so that no identification inferences could be made.

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

The ABA notes the Government's flagged intent to introduce a proportionate compliance framework and desire to reasonably limit penalising victims of cyber incidents. Considering this, the ABA believes, at least initially, consequences other than civil penalties should be adopted (e.g. infringement notice, public notice).

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

The ABA acknowledges that greater visibility of ransomware incidents requires a degree of detail and timeliness in reporting, however, it may not be necessary for ransom payment related information to be disclosed in any public reporting. Disclosure of such information risks setting precedents on making payments (e.g. normalising payments in certain industries) and may embolden threat actors further – particularly where a specific industry is perceived as more likely to pay. Ransom payments are highly complex and carry deep connotations, which if disclosed could additionally undermine public trust in the entity or industry.

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

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

[5] Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496 (ASIC v RI Advice)

The consultation has referenced 'consequence management' in its list of permitted uses. While more specific commentary on consequence management has been provided in the response to *Measure 6*, the ABA is concerned that consequence management does not appear congruent to the purpose of encouraging greater information sharing, nor likely to promote confidence under a limited use obligation.

While cognisant that it is not necessarily possible to envisage all uses required of information in a future hypothetical cyber incident, the proposed scope of permitted uses is extremely broad – making it challenging to reasonably consider potential impacts. Of additional concern is the risk that during an incident, the expansive permitted uses could lead to information being shared across agencies rapidly – undermining the purpose of the policy. The ABA recommends greater detail be provided on the specific types of information to be gathered and their subsequent permitted use cases.

The ABA supports assessment of relevant models overseas as a point of comparison. For example, the US Cyber Security Information Sharing Act (CISA) limits use of cyber security information (i.e., cyber threat indicators and defensive measures) to a 'cybersecurity purpose'[6], preventing its usage in regulatory enforcement purposes.

18. What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?

Greater information flows between industry and the ASD/Cyber Coordinator are an important enabler of a more cybersecure Australia. These information flows are best enabled by an ecosystem that promotes deep partnerships between parties and incentivises maximum intelligence sharing, while managing the risk inherent in sharing sensitive information.

A key risk emerges where sensitive information has the potential to be disclosed to government bodies or regulators beyond the ASD or Cyber Coordinator. Constraints on usage should align with how information flows to third parties, including restrictions on protected and/or sensitive data.

Information exchanged with other regulators should focus solely on cyber threat intelligence pertinent to their respective sectors. Such data should be utilised exclusively for addressing cybersecurity threats and not for regulatory enforcement actions.

19. What else can Government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?

The ASD and ACSC play a critical role in the immediate aftermath of an incident, a role which is supported by timely and quality information. While strongly supportive of this engagement, the ABA acknowledges the material business risks that occurring when highly sensitive and/or legally privileged information is shared between parties.

While *Measure 3* seeks to address these concerns it is not apparent how in practice such safeguards would be established. The ABA recommends that additional detail be provided to detail how / when information would be shared beyond the ASD/ACSC, and whether consent would be obtained from the organisation when information is shared.

While the proposal indicates that information pertaining to the incident shared with government could not be used for compliance activities, it is unclear in practice how these restrictions would be implemented, and to what extent they would provide relief against the same information subsequently being obtained by a regulator and used for enforcement activity. Even where only

[6] Meaning the purpose of protecting an information system or information from a cybersecurity threat or security vulnerability.

partial information is shared beyond the ASD/ACSC, there are risks the knowledge of sensitive information could be easily imputed, enabling compliance activity. Simply put, it is uncertain how the obligation of limited use, as proposed, would provide any relief from a regulator who gains knowledge of information provided under limited use from using its other powers to obtain the identical information for investigation or compliance purposes. The consultation paper illustrates this challenge[7], suggesting that the ASB and Cyber Coordinator could use gathered information for industry guidance etc. but not for investigation or compliance.

A further complication arises when considering that cyber incident data could be bound by contractual limitations and/or constitute the confidential information of external parties. Sharing such information represents a clearly unacceptable risk and as such entities should be granted immunity from civil liability if they share cyber incident data and subsequently encounter contractual or legal repercussions from third parties for its disclosure.

It is suggested that consideration be given to how models in comparable countries are structured to see where best practice design principles can be leveraged. The Cyber Security Information Sharing Act (CISA) in the United States offers various safeguards to entities that share cybersecurity information within the CISA framework. These protections encompass immunity from liability concerning the divulgence of such information, preservation of privileges such as legal professional privilege, and exemption from disclosure under Freedom of Information (FOI) laws.

To support further engagement on this proposal, the ABA seeks clarification on the following key questions:

- How would this information be quarantined from investigation and compliance activities?
- How would information be treated in the event of regulators becoming involved in incident management?
- Information provided during an incident is often incomplete and/or inaccurate, requiring further time to verify. What safeguards would be established to protect against dissemination of incomplete information?
- What principles would guide the storage and retention of information?

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

20. What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?

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

22. How should a CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?

23. What factors would make a cyber incident worth reviewing by a CIRB? 24. Who should be a member of a CIRB? How should these members be appointed?

25. What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?

26. How should the Government manage issues of personnel security and conflicts of interest?

27. Who should chair a CIRB? 28. Who should be responsible for initiating reviews to be undertaken by a CIRB?

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

[7] Consultation paper page 20

30. To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?

31. What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?

32. What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?

33. What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?

The ABA supports the objective of retrospective incident analysis as a vital tool to improve Australia's cyber security environment. The CIRB will be most effective under a model of close collaboration and partnership with industry to drive capability uplift, as opposed to driving resources towards additional compliance activity. Therefore, the CIRB's powers should be voluntary, and that the information provided by entities to it be protected under similar confidentiality and limited-use restrictions to other information flows to government (e.g. ACSC).

CIRB Scope

In principle a CIRB would require transparent and prescriptive guardrails to guide what types of artefacts would be produced, and the processes underpinning their production and (potential) dissemination. The ABA supports minimising duplication across regulators (e.g. APRA, ASIC, OAIC), so that the scope of the proposed CIRB does not interfere with existing investigatory powers that regulators would deploy in assessing the cause and impact of an incident.

Reflecting concerns raised in Measures 2 and 3, there is a hypothetical risk that analysis and insights generated by any artefacts could enable inferences to be made against individual entities, triggering investigation and compliance activity, while undermining the objectives and confidence in such a review mechanism. Therefore, appropriate mechanisms should be put in place to ensure that the CIRB does not interfere with enforcement or regulatory action. For example, CIRB reports and recommendations should not be admissible in legal proceedings. The CIRB's scope could address these issues either through limiting root cause analysis, or through adjusting outputs so that the inferences could not be made (e.g. sufficiently generalised root causation).

To further maintain confidentiality and industry confidence, the ABA endorses sensible measures to aggregate and deidentify data. Regular publication, as opposed to ad-hoc reporting, may be a pragmatic model to further limit data inferences. It is also suggested that any hearings undertaken during an investigation confidentially.

To further protect confidentiality, the ABA recommends consideration of the following:

- Establishing protections related to aggregating and anonymising reported information for the purpose of sharing information with the public and/or government agencies.
- Assessment of the applicability and potential exclusion from the FOI regime of information shared in a 'no fault' scenario – reflecting practices in certain foreign jurisdictions.

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

34. How are you currently managing risks to your corporate networks and systems holding business critical data?

Entities regulated by APRA must comply with multiple regulations, including CPS 234, which mandates various protective measures for their Information Assets. The definition of 'information asset' under CPS 234 is broad, encompassing data whose compromise could impact the entity

financially or otherwise, as well as the interests of depositors, policyholders, beneficiaries, or other customers. This extends to both operational and non-operational business data. CPS 234 additionally obliges entities to promptly notify APRA upon discovering significant information security incidents or weaknesses in controls related to their Information Assets.

To prevent regulatory overlap, the ABA strongly urges any additional measures concerning the regulation of non-operational data in the SOCI Act should apply only to responsible entities not already subject to a commensurate regulatory framework already.

35. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?

The suggested revisions should not inadvertently extend to responsible entities where there are overlapping regulatory frameworks, such as prudential standards like CPS 234.

36. What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

Ambiguity

Given overlap between and potential interchangeable usage between 'data storage systems' and 'data processing services', clarification on what is precisely captured by a 'data processing service' is required to consider this further.

Presently, the SOCI Act mandates responsible entities for Critical Infrastructure (CI) assets to notify providers of data storage and processing services when handling the entity's business-critical data, with civil penalties for non-compliance. While the concept of data storage providers is generally understood, there lacks precise guidance or definition for a 'data processing service'. This ambiguity makes it challenging for responsible entities to discern when they are engaging with a data processing service regulated by the Act – vital to understand correctly given the potential for civil penalties.

Concerning data located outside Australia, the SOCI Act doesn't classify an asset as a CI asset if it's situated beyond Australian borders. If a responsible entity stores business-critical data outside Australia, would the proposed reforms, along with any new obligations regarding the security of that data, cease due to its location? Under SOCI, obligations already extend to all assets "used in connection with the 'banking business'," encompassing assets that hold 'business-critical data'. Consequently, it may not be necessary to include data storage systems holding 'business-critical data' in the definition of 'asset'.

Compliance burden

There's a potential expansion of restrictions regarding the handling of protected information to encompass matters concerning non-operational data and data storage systems. For instance, documents or information related to corporate/non-operational data storage systems incorporated into critical infrastructure management programs would be subject to the restrictions outlined in Part 4 of the SOCI Act. This extension of restrictions imposes a significant compliance burden.

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

37. How would the proposed directions power assist you in taking action to address the consequences of an incident, such as a major cyber-attack on your critical infrastructure asset?

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

39. What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

In principle, the ABA acknowledges the intent behind the proposal for establishing consequence management powers, insofar as that they provide a power of last resort to support individuals and businesses to recover from cyber security incidents.

However, the ABA holds deep concern over the extent of reserve powers being proposed under *Measure 6*. It is noted that for entities already regulated under Part 3A of the SOCI Act, this represents a significant increase in the scope of directions powers, far beyond technical incident management and triage.

To support further consideration, the ABA requests additional detail be provided to address:

- The precise nature of problems being solved through the proposal, including specific legislative gaps to be closed. While some historical examples have been provided, the proposal through its 'catch-all' nature does not appear to be designed specific to these challenges. Without additional detail, it is difficult to assess whether a need for these powers exists, and if the proposed powers are appropriate to address these problems. E.g., is the issue with industry coverage of powers, the breadth of powers, harmonisation of powers?
- Disproportionality between the intended issues to be remedied and the expansive powers proposed. This may add further complexity to an entity's ability to assess the potential consequences. Compounding this is the challenge of managing real-time incidents, where information is incomplete and changes rapidly[8], increasing the likelihood of unintended consequences.

The ABA understands from engagement with Home Affairs to date that the powers are by design widely scoped to maximise the likelihood of their applicability to unknown future incidents.

Notwithstanding concerns over limitation of scope, the ABA strongly supports further consideration of the following areas.

<u>Definition</u>

- The consultation has provided detail to the scope and context of consequence management, however the concept itself is still ambiguous. The provision of a more codified and precise definition of consequence management is recommended to facilitate greater certainty of scope.

<u>Objectives</u>

- It is recommended that a concise summary of the objectives of consequence management powers is prepared. The current level of detail on objectives (e.g., addressing prejudice of socioeconomic stability) is extremely vague and could introduce unnecessarily wide scope and discretion.
- In principle, the ABA recommends the scope of directions to be general as opposed to specific – preserving the directional intent of the regime, without prejudicing a business' autonomy to manage the holistic incident. For example, this could involve directions to

[8] Known as the 'fog of war'

'*strengthen cybersecurity controls to respond to the vulnerability'* compared with more prescriptive directions to *'upgrade a specific system'.*

Information gathering

- It is recommended that limitations on purpose and usage are placed on any information gathered, similar to the guardrails outlined in *Measures 2 and 3*.

Costs

- It has not been made clear how the costs incurred through complying with directions would be considered. The proposals suggest that any third party, regardless of fault could be subject to a direction if the incident necessitated it. Compliance with such directions, particularly where customer data or triaging is required, can be both resource intensive and costly. We recommend additional consideration be given to how determination of fault would be made, and how/if this would be considered when directions were issued to third parties to the incident.
- A suggestion for consideration to minimise potential cost impacts could be implementing guardrails over directions issued to third parties during an incident. E.g. principles established to minimise the scope of potential directions made to third parties.

Guardrails

- The expansive nature of the proposed powers should be accompanied by a commensurate framework to determine how and when they could be used. It is recommended that greater detail be provided on what thresholds would apply when considering the application of powers. E.g. in the case of 'socioeconomic prejudice', it is unclear how this would be assessed. Would there be a quantitative threshold? What level of impact would meet this threshold? How would this threshold be determined?

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

40. How can the current information sharing regime under the SOCI Act be improved?

The SOCI Act imposes a general prohibition on the recording, disclosure or use of protected information by any person or organisation. Safeguarding protected information is fundamental, however there are concerns that ambiguity in the current provisions adversely affect the ability of responsible entities and the government to manage crisis incidents. It is welcomed that these concerns have been acknowledged by Government in this consultation.

The existing information sharing regime could be enhanced through the following measures:

- Elimination of criminal liability for certain violations of the protected information provisions. Instead, imposing civil penalty provisions might be a more fitting sanction, especially concerning an entity's management of information pertaining to its own critical infrastructure assets.
- Reducing the constraints on the internal utilisation and documentation of protected information by an entity, prioritising instead restrictions on its disclosure to third parties.

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

Greater clarity and flexibility are sought regarding the restrictions and exceptions applicable to protected information. The ABA is concerned that current provisions introduce ambiguity and complexity into how an entity makes decisions concerning the storage, utilisation, and disclosure of information pertaining to its critical infrastructure assets. During incident management, such ambiguity becomes particularly problematic.

Additionally, further information is required regarding the harm-based assessment to evaluate its potential impact. If implemented, additional regulatory guidance would be necessary to assist entities in applying the test, considering its complex factors such as socioeconomic stability, national security, and defence of Australia. It's worth noting that the introduction of such a test would likely increase compliance burdens, including the establishment of internal processes to manage and document the harms-based assessment.

For critical infrastructure providers there is additional ambiguity regarding the intersection of SOCI Act requirements and the FOI Act. The SOCI Act may necessitate entities to share highly sensitive information with various government and regulatory agencies, potentially leading to further disclosure to other agencies without the entity's knowledge. While public access to this information falls under the FOI Act, the FOI Act does not currently classify protected information under the SOCI Act as an exempt document for FOI purposes. The ABA seeks clarification on how this risk would be mitigated and would support in principle appropriate legislative reforms to address this. For example, amending the FOI Act to designate any documents containing protected information under the SOCI Act as exempt documents under section 38 of the FOI Act, akin to the protection provided to 'protected documents' or 'protected information' in section 56(11) of the Australian Prudential Regulation Authority Act 1988 (Cth).

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

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

Proposed reforms should not be designed agnostic of existing regulatory obligations. Regarding the suggested review and remedy power, further clarification is needed regarding whether these obligations solely persist for entities not presently mandated to provide a Risk Management Plan (RMP) under the SOCI Act. If the objective is to extend the obligation to encompass all critical assets regardless, it's essential to assess whether existing regulations serve a similar purpose.

For instance, banking and financial services regulations, such as CPS 220 and CPS 234, already address adequate risk management practices and cybersecurity, possessing comparable powers to those proposed. The prudential regulator possesses various enforcement mechanisms, including directive powers and the imposition of financial penalties like regulatory capital for deficient risk management systems. These measures are applied commensurate with the significance of the deficiency and the organisation's scale within Australia's banking and financial system, a significant sector under the SOCI framework.